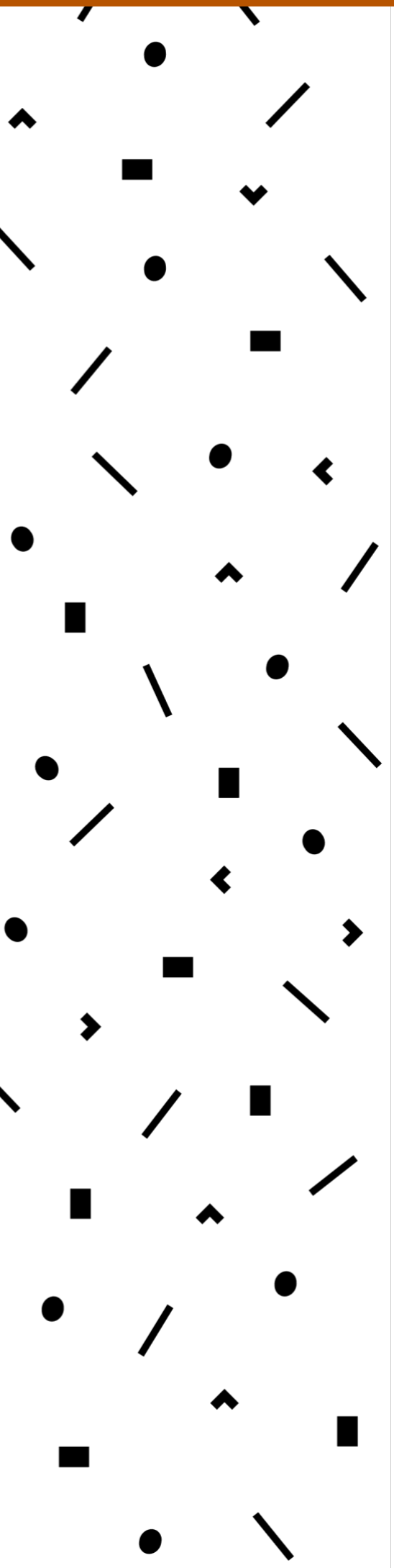


LAMK
Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

SEURAAVAN SUKUPOLVEN PALOMUURIN VALINTA

LAHDEN AMMATTIKORKEAKOULU
Insinööri (AMK)
Tieto- ja viestintätekniikka
Tietoverkot
Syksy 2018
Tuomaala Jirko

Tiivistelmä

Tekijä(t)	Julkaisun laji	Valmistumisaika
Tuomaala, Jirko	Opinnäytetyö, AMK	Syksy 2018
	Sivumäärä	
	37	

Työn nimi

Seuraavan sukupolven palomuurin valinta

Tutkinto

Insinööri (AMK)

Tiivistelmä

Seuraavan sukupolven palomuuri on kolmannen sukupolven palomuuriteknologiaa, joka yhdistää perinteisen palomuurin ominaisuudet sovellustunnistukseen perustuvaan suojaan. Seuraavan sukupolven palomuurit sisältävät myös muita tietoturvasovelluksia kuten esimerkiksi virustorjunnan ja tunkeilijanestojärjestelmän.

Opinnäytetyön tavoitteena oli löytää Lahden ammattikorkeakoululle uusi palomuuri vertailemalla vaihtoehtoja kilpailutusta varten. Vertailuun valittujen palomuurien piti täyttää tietyt ehdot. Ennakkoon oli tutustuttu Palo Alto Networksin palomuureihin ja valittu potentiaaliseksi vaihtoehdoksi PA-5220. Vertailuun valittiin laitteita kolmelta muulta laitevalmistajalta, jotka olivat Cisco, Check Point ja Sophos.

Internetin liikenteen muutos on pakottanut palomuurin kehittymistä. Nykyään liikenteen suodattaminen pelkillä IP-osoitteilla, porteilla ja protokollilla ei ole enää etenkään isoimmissa verkkoympäristöissä täysin turvallista. Esimerkiksi verkkoliikenteen salaus on johtanut siihen, että palomuurien on pystyttävä purkamaan SSL-salauksia pakettien tarkastusta varten.

Vertailuosuudessa tutustuttiin eri laitevalmistajien seuraavan sukupolven palomuurien toimintatapoihin, suorituskykyyn sekä hintoihin. Vertailussa pohdittiin myös laitevalmistajien mainetta ja luotettavuutta alalla.

Vertailun avulla sopivimmaksi laitteeksi valittiin Palo Alto Networksin PA-5220 -palomuuri. PA-5220 pärjäsi vertailussa etenkin selkeiden ja laajojen markkinointimateriaaliensa ansiosta. Palo Alto Networks on myös hyvämaineinen yritys seuraavan sukupolven palomuurien tuottajana.

Asiasanat

Seuraavan sukupolven palomuuri, NGFW, tietoturva, vertailu

Abstract

Author(s)	Type of publication	Published
Tuomaala, Jirko	Bachelor's thesis	Autumn 2018
	Number of pages	
	37	

Title of publication

Next-Generation Firewall Selection

Name of Degree

Bachelor of Engineering

Abstract

Next-Generation Firewalls are third generation of firewalls which contain features from basic firewalls adding new filtering methods like application identification. NGFWs can have also other security applications like Antivirus and Intrusion Prevention System.

The aim of the thesis was to find a new Next-Generation Firewall for Lahti University of Applied Sciences by comparing different products from multiple vendors. Palo Alto Networks' firewalls were explored in advance and potential model for our purposes was PA-5220. In comparison, there were also firewalls by Cisco, Check Point and Sophos.

The thesis begins by studying the history of firewalls and how they have developed. The change of internet traffic has forced firewalls to develop more secure. Nowadays filtering traffic with IP-addresses, protocols and ports is not very effective anymore in a big environment.

The later part of the thesis contains a firewall comparison. Three main things in comparison were specifications, prices and how certain features are implemented.

The winner of the comparison was Palo Alto Network PA-5220 firewall. PA-5220 was good in several technical areas and its price was under the average. Palo Alto Networks also offers extensive documentation of their firewalls on their website. They are also a reputable company in firewall business.

Keywords

Next-Generation Firewall, NGFW, information security, comparison

SISÄLLYS

1 JOHDANTO

Palomuuri on tärkeä osa tietoverkkoa. Jos laite yhdistetään internetiin, tarvitaan lähtökohtaisesti aina palomuuri. Verkkohyökkäyksistä on tullut ajan myötä ammattimaisempia ja kohdistetumpia, jossa hyökkääjillä on selkeä päämäärä. Nykypäivänä hyökkääjien yksi suurimpia motiiveja on raha, jota hyökkääjät voivat saada esimerkiksi kiristysohjelmien avulla. Hyvän palomuurin hankkiminen voi parantaa verkkoympäristön tietoturvaa ja minimoida riskejä huomattavasti.

Tämän opinnäytetyön tavoitteena on valita seuraavan sukupolven palomuuri Lahden ammattikorkeakoululle. Opinnäytetyössä tutustutaan seuraavan sukupolven palomuurien toimintaan ja niiden olennaisimpiin ominaisuuksiin. Tutkimusosassa käydään myös läpi palomuurin kehityksen vaiheet ja selvitetään, mikä on ajanut palomuurien kehitystä eteenpäin.

Työvaiheessa tehdään vertailu eri laitevalmistajien palomuurilaitteiden välillä kilpailutusta varten. Vertailu tehdään suorituskyvyllisten ominaisuuksien ja listahintojen avulla. Vertailussa tarkastellaan myös eri laitevalmistajien tapoja erilaisten ominaisuuksien toteuttamiseen ja pohditaan muita palomuurin valintaan liittyviä seikkoja.

2 PALOMUURIN TOIMINTA

Palomuuri on tietoverkossa toimiva järjestelmä, jonka tehtävänä on suodattaa sisään- ja ulospäin meneviä tietoliikenneyhteyksiä ennalta määrättyjen sääntöjen avulla. Yleisin palomuurin tehtävä on torjua ulkoverkosta tulevia hyökkäyksiä sisäverkkoon. Palomuurit voidaan jakaa karkeasti kahteen pääryhmään: laitepalomuureihin ja sovelluspalomuureihin. Laitepalomuurien tehtävä on suodattaa liikennettä kahden tai useamman verkon välillä. Tällainen palomuuri toimii täysin omana laitteenaan verkossa tai se on voitu yhdistää esimerkiksi osaksi reititintä. Laitepalomuurien toiminta voi muistuttaa ylipäätään paljon reitittimen toimintaa, koska ne jakavat paljon samoja toimintoja keskenään. Laitepalomuuri voidaan usein määritellä esimerkiksi DHCP- (Dynamic Host Configuration Protocol) tai VPN (Virtual Private Network) -palvelimeksi. Tämä opinnäytetyö perehtyy laitepalomuureihin. (Rouse, Clark & Cobb 2018.)

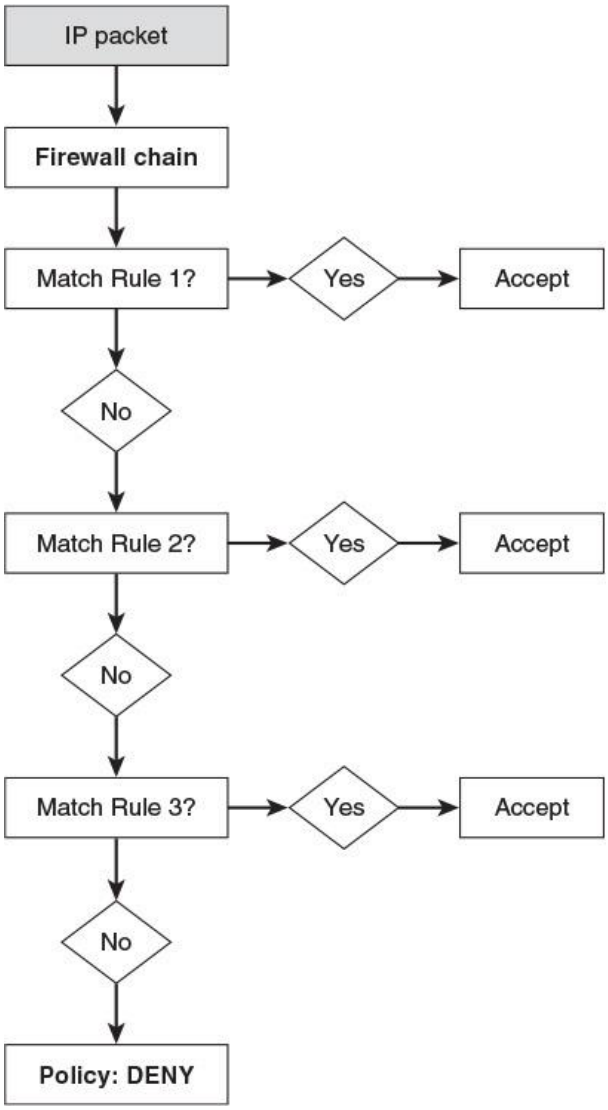
Sovelluspalomuurit ovat ohjelmistoja, jotka toimivat käyttäjän päätelaitteella kuten tietokoneella, jossa ne suodattavat liikennettä käyttäjän laitteen ja verkon välillä. Niiden suurin ero laitepalomuureihin on se, että ne suodattavat sisään- ja ulospäin kulkevaa liikennettä pelkästään sillä laitteella, johon palomuuri on asennettu. Ne voivat kuitenkin estää käyttäjän laitetta saamasta tartuntaa ja estää tartunnan saaneen laitteen levittämästä haittaohjelmaa eteenpäin. Nykyään esimerkiksi Windows- ja MacOS-käyttöjärjestelmissä on esiasennettu palomuuriohjelmisto. (Tech-FAQ 2018.) Näihin järjestelmiin on mahdollista myös asentaa kolmannen osapuolen palomuuriohjelmistoja (Marshall & Ellis 2017).

2.1 Tilaton palomuuri

Tilaton palomuuri (Stateless Firewall, Packet-filtering Firewall) on ensimmäisen sukupolven palomuuri, joka on toimintatavoiltaan yksinkertaisin. Tilattoman palomuurin toiminta perustuu pääsylistoihin (Access Control List, ACL), joiden avulla palomuuri suodattaa paketteja. Pääsylistaan kirjataan säännöt, joita palomuurin halutaan noudattavan. Pääsylista toimii ylhäältä alaspäin, jota havainnollistetaan kuviossa 1. Palomuuri vertaa tulevan tai lähtevän paketin otsikkoa pääsylistan sääntöihin rivi riviltä, minkä jälkeen paketti joko päästetään läpi tai hylätään. Palomuuri tarkastelee paketin otsikosta viittä tietoa: IP-lähdeosoitetta, lähdeporttia, IP-kohdeosoitetta, kohdeporttia ja IP-protokollaa (TCP tai UDP). Jos määritelty sääntö pätee pakettiin ennen listan loppua, ei palomuurin tarvitse käydä koko listaa läpi. Pääsylistassa ylempänä määritelty sääntö

yliajaa aina sen alapuolella olevat säännöt. Tämän takia pääsylistassa olevien sääntöjen järjestyksellä on väliä. (Suehring 2015.)

Usein pääsylistat konfiguroidaan siten, että kaikki määrittelemätön liikenne estetään. Tätä tekniikkaa käytetään myös kuviossa 1. Tämä tarkoittaa, että jokainen haluttu läpi pääsevä yhteystyyppi pitää määritellä erikseen. Tällöin määrittelemättömän liikenteen estävä sääntö laitetaan listan viimeiseksi (kuviossa 1 alimpana). Jos tämä sääntö määriteltäisiin pääsylistassa ensimmäisenä, se estäisi kaiken liikenteen. Tätä tekniikkaa kutsutaan valkolistaukseksi (white-listing). Valkolistauksen suurin etu on tietoturvallisuus, mutta sen ylläpitäminen voi olla työläämpää. Valkolistaus on yleisempi tapa ylläpitää palomuuria. (Suehring 2015.)



KUVIO 1. IP-paketin kulku pääsylistan läpi (Suehring 2015)

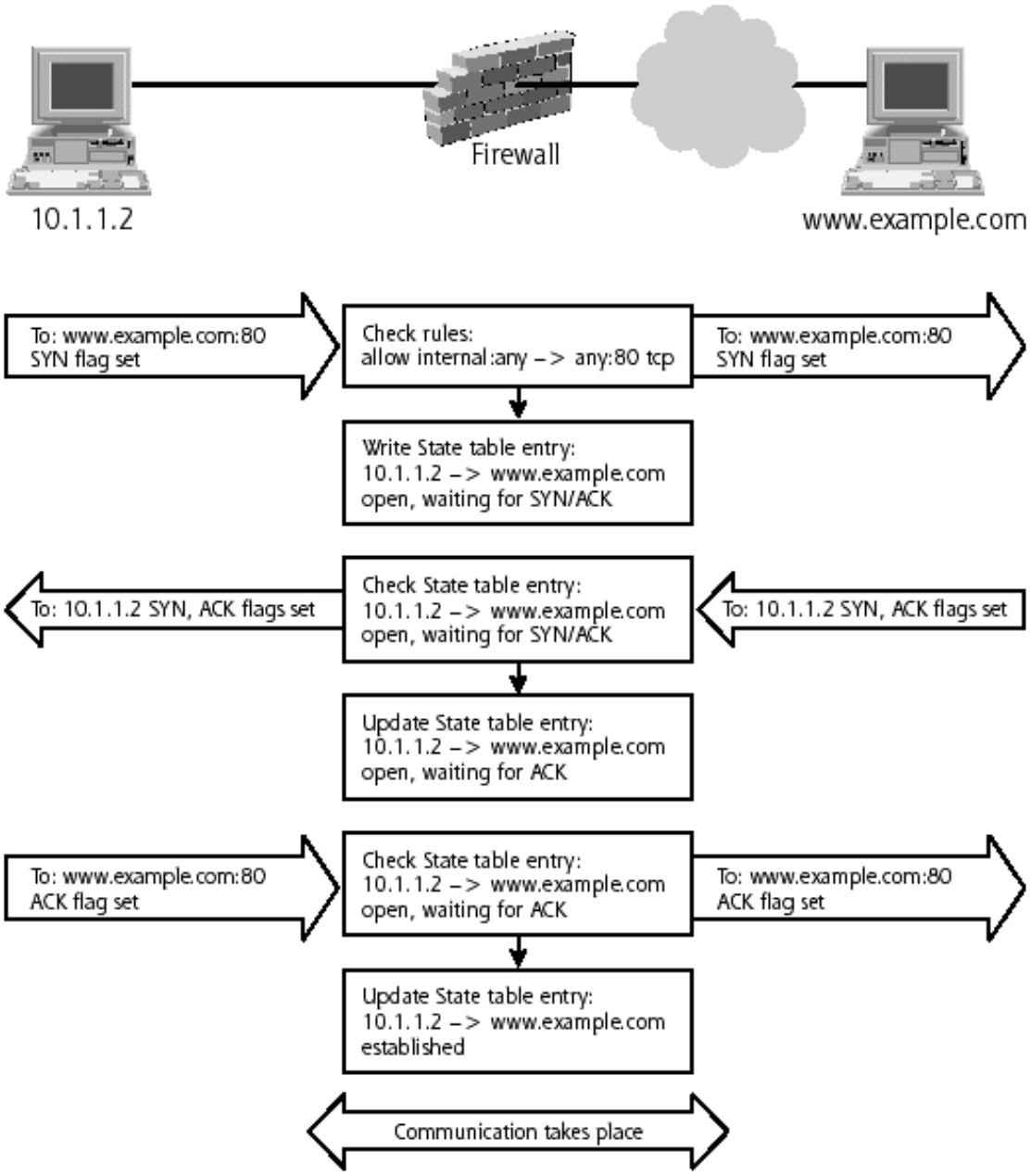
Valkolistauksen vastakohta on mustalistaus (black-listing), jossa oletuksena kaikki liikenne sallitaan ja ei-halutut yhteydet estetään. Tämä on tietoturvan kannalta huonompi vaihtoehto, mutta sitä voi olla helpompi ylläpitää. (Suehring 2015.)

2.2 Tilallinen palomuuri

Tilallinen palomuuri on toisen sukupolven palomuuriteknologiaa, missä palomuuri seuraa verkkoyhteyksien toimintatilaa ja ominaisuuksia. Sen toiminta perustuu ominaisuuteen, jossa palomuuri tietää yhteyden tilan ja tekee päätöksen paketin hyväksymisestä tai hylkäämisestä. Vain tiedetyt aktiiviset yhteydet voivat läpäistä palomuurin. Tätä toimintaa kutsutaan tilalliseksi paketin tarkastukseksi (Stateful Packet Inspection, SPI) tai dynaamiseksi pakettisuodatukseksi (Dynamic Packet Filtering). Tilallinen palomuuri sisältää myös tilattoman palomuurin ominaisuudet, jolloin paketin lähtiessä tai saapuessa sen on ensin läpäistävä pääsylistan säännöt. Jos paketti pääsee tilattoman tarkastuksen läpi, tarvitaan tilallista paketin tarkastusta. (Yeo 2003.)

Yksinkertaisin tapa havainnoida tilallista paketin tarkastusta on käyttää TCP (Transmission Control Protocol) -yhteyttä, jonka kulkua palomuurin läpi on havainnollistettu kuviossa 2. TCP-yhteydessä on kolme vaihetta, joihin sisältyvät yhteyden muodostaminen (SYN), tiedonsiirto (SYN/ACK) ja yhteyden katkaisu (ACK). Tätä prosessia kutsutaan kolmitiekättelyksi (3-way-handshake). Tilallinen paketin tarkastus käyttää tilan tarkasteluun lähde- ja kohdeosoitteita, portteja sekä TCP-yhteyden lippuja (flag) ja järjestysnumeroa. TCP-lipusta nähdään suoraan yhteyden tila. Järjestysnumeron avulla voidaan estää esimerkiksi palvelimen lähettämästä väärää tai haitallista ACK-pakettia käyttäjälle. Se osaa avata tarvittavat portit palomuurista yhteyden muodostamiseksi. Tilattomassa palomuurissa järjestelmään palaaville paketeille on avattava portti manuaalisesti. Kuviossa 2 käyttäjä ensiksi yhdistää palvelimeen hakeakseen verkkosivuun www.example.com käyttäen porttia 80. Tällöin alkaa TCP-yhteyden ensimmäinen vaihe; SYN-lipun asettaminen. Palomuuri tarkastaa, että lähetetty paketti noudattaa pääsylistaan määriteltyjä sääntöjä ja päästää paketin eteenpäin palvelimelle. Samalla palomuuri kirjoittaa tilataulukkoon (State table) tiedon, että yhteys on auki, ja että palomuuri odottaa SYN/ACK-pakettia vastauksena palvelimelta. Palvelin vastaa käyttäjän lähettämään pyyntöön nyt SYN/ACK-paketilla. Palomuuri tarkastaa tilataulukosta, että paketin otsikon tiedot täsmäävät edelliseen vaiheeseen ja päästää paketin läpi käyttäjälle. Samalla palomuuri päivittää tilataulukkoon tiedon, että SYN/ACK-paketti on mennyt läpi käyttäjälle, ja nyt odotetaan käyttäjän vastaavan vielä ACK-

paketilla. Käyttäjä lähettää ACK-paketin palvelimelle, ja palomuuri tarkastaa tilataulusta sen yhteensopivuuden ja päästää paketin läpi. (Yeo 2003.)



KUVIO 2. TCP-yhteyden kulku palomuurin läpi tilataulukon avustuksella (Yeo 2003)

3 SEURAAVAN SUKUPOLVEN PALOMUURI

Seuraavan sukupolven palomuuri (Next-Generation Firewall) on kolmannen sukupolven palomuuriteknologiaa, joka yhdistää edellisten palomuurisukupolvien ominaisuudet sovellustunnistukseen perustuvaan suojaan. Seuraavan sukupolven palomuurit sisältävät myös muita tietoturvaa parantavia ominaisuuksia, kuten pakettien syvätarkastuksen (Deep Packet Inspection) tai tunkeutujanestojärjestelmän. (Rouse & Shea 2018.) Ennen Next-Generation palomuureja perinteisten palomuurien puutteita korjattiin erillisillä verkkoon asennetuilla tietoturvasovelluksilla. Ne toimivat verkossa joko omina laitteinaan tai keskitetysti yhdessä laitteessa. Tällaista suojaustapaa kutsutaan nimellä Unified Threat Management (UTM). UTM-laitteilla on kuitenkin ongelma, että ne ovat selvä pullonkaula sisäverkossa. Ne saattavat myös ruuhkauttaa sisäverkkoa, kun erilliset tietoturvasovellukset toimivat omina laitteinaan. Seuraavan sukupolven palomuurit yhdistävät UTM-sovellukset suoraan palomuuriin. (Li & Clark 2015, 15.)

Seuraavan sukupolven palomuuria on tästä huolimatta hankala määritellä yksiselitteisesti, koska eri laitevalmistajat tarjoavat omiin palomuureihinsa erilaisia ominaisuuksia vaihtelevilla toteutustavoilla. Seuraavan sukupolven palomuurit ovat myös kehittyneet niiden alkuajoista. Kansainvälinen ICT-alan tutkimus- ja konsultointiyritys Gartner määritteli ensimmäisen kerran, että seuraavan sukupolven palomuuriksi luokiteltavan palomuurin tulee pystyä tunnistamaan sovellustason hyökkäykset, valvomaan sovellustason sääntöjä ja tutkia ja purkaa SSL-salattua liikennettä. Siinä tulee myös olla kaikki perinteisen palomuurin valmiudet ja sisältää kaikki ominaisuudet tunnistepohjaisesta tunkeutumisenestojärjestelmästä. (Li & Clark 2015, 14-15.)

Modernit tartunnat, kuten web-pohjaisilla haittaohjelmilla tehtävät hyökkäykset, kohdennetut hyökkäykset ja sovellustason hyökkäykset, ovat pakottaneet palomuurin kehittämistä entisestään. Seuraavan sukupolven palomuuri suorittaa huomattavasti syvemmän tarkastelun verrattuna tilalliseen tarkasteluun. Siinä tarkastetaan myös paketin hyötykuorma ja yhtenevät tunnistetiedot haitallisille aktiviteeteille, kuten hyökkäyksille ja haittaohjelmille. Perinteisissä palomuureissa säännöt luodaan usein siten, että oletetaan tiettyjen sovellusten toimivan aina samassa portissa. Haitallinen sovellus on voitu sulkea pois estämällä käyttäjältä tietyt portit ja protokollat. Nykyään monet sovellukset (esimerkiksi pikaviestisovellukset tai web-pohjaiset sovellukset) voivat toimia porteissa, joiden estäminen saattaisi aiheuttaa ongelmia muiden palveluiden käytössä. Esimerkiksi monet verkkosivuilla toimivista sovelluksista käyttävät portteja 80 ja 443, jotka ovat olennaisimpia portteja internetin käytössä. Myös hyökkäykset voivat naamioitua muuksi liikenteeksi. Tästä syystä suojaus pelkkien porttien, protokollien ja IP-osoitteiden avulla ei

ole enää luotettavaa ja kannattavaa. Tämä on johtanut identiteettiin perustuvan turvan kehittämiseen. (Sweeney 2012.)

Seuraavan sukupolven palomuurin tavoite on estää OSI-mallissa (kuvio 3) kerroksien 4-7 (kuljetus, istunto-, esitystapa- ja sovelluskerros) kohdistuvien hyökkäyksien kasvava määrä sisällyttämällä OSI-mallin kerroksia palomuuriin, jolloin parannetaan verkkoliikenteen suodatusta, joka on riippuvainen paketin sisällöstä. (Rouse & Shea 2018). Aiemmat palomuuriteknologiat ovat suodattaneet liikennettä kerroksissa kolme (verkkokerros) ja neljä (kuljetuskerros). (Davis 2009).

KUVIO 3. OSI-malli (Wikipedia 2018)

Seuraavan sukupolven palomuuri tarjoaa ylläpitäjälle paremman valmiuden ja kontrollin yksittäisiä sovelluksia kohtaan syvemmän tarkastelukyvyn ansiosta. Ylläpitäjä voi esimerkiksi luoda hyvinkin suoraviivaisia sääntöjä, joilla voidaan kontrolloida verkkosivuja ja sovelluksia verkossa. (Sweeney 2012.)

3.1 Sovellustunnistus

Sovellustunnistus (Application Awareness) on seuraavan sukupolven palomuurin olennaisin ominaisuus. Sovellustunnistus antaa ylläpitäjälle mahdollisuuden nähdä sovellukset, joita käytetään verkossa, sekä mahdollisuuden kontrolloida niitä. Palomuuri voi oppia sovellusten toimintatapoja, käyttäytymistä, ominaisuuksia ja mahdollisia riskejä.

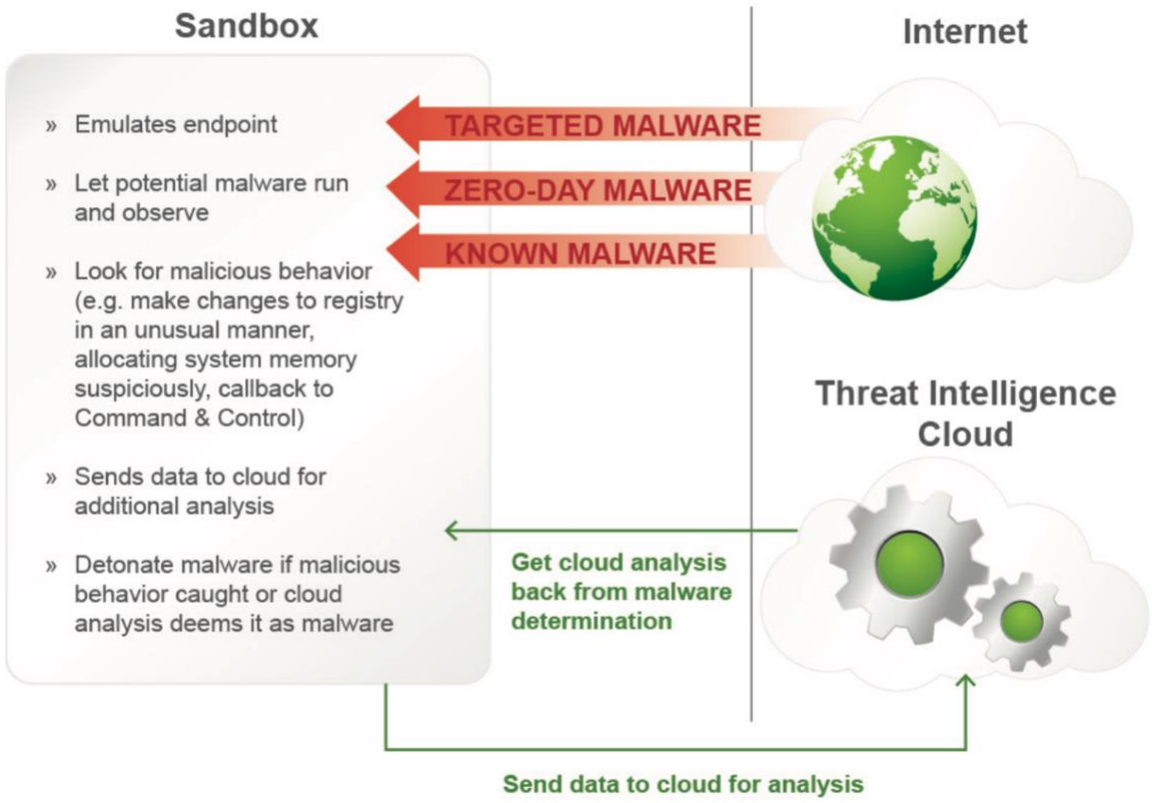
Palomuuri käyttää useita keinoja sovelluksien identifioimiseen, jonka avulla voidaan hahmottaa sovelluksien rakenne, osa-alueet ja aliohjelmat. Identifioimisen avulla voidaan estää tai sallia näitä tiettyjä osa-alueita tai alisovelluksia. Palomuuri voi esimerkiksi sallia vain hyväksytyt Office 365 -tunnukset tai vaikkapa sallia Slackin pikaviestimiseen, mutta estää siinä tiedostojen lähetys. (Palo Alto Networks 2018b.)

3.2 Sisällöntunnistus

Sisällöntunnistus on myös yksi osa seuraavan sukupolven palomuurin ominaisuuksia. Se voi sisältää useita erilaisia tekniikoita, joilla torjutaan uhkia ja hallitaan sisältöä verkossa. Ne ovat usein erilaisten lisenssien alaisia ominaisuuksia, eikä niitä ole automaattisesti mukana palomuurissa. Tällaisia ominaisuuksia ovat esimerkiksi tunkeilijanestojärjestelmä, virustorjunta, URL-suodatus sekä tiedosto- ja datasuodatus. (Palo Alto Networks 2018c.)

3.2.1 Uhkien torjunta ja sandboxing

Uhkien torjunta on toteutettu seuraavan sukupolven palomuureissa usein sandboxing-tekniikan avulla, jota havainnollistetaan kuviossa 4. Sandbox on turvallinen eristetty virtuaaliympäristö, joka on suunniteltu muistuttamaan käyttäjän toimintaympäristöä. Sandbox-ympäristössä palomuuri voi avata epäilyttäviä tiedostoja ja sovelluksia sekä ajaa koodia. Tämän jälkeen tiedostoja ja sovelluksia tarkkaillaan haitallisen toiminnan varalta. Haitallinen toiminta voi esiintyä esimerkiksi järjestelmän rekisterimuutoksina. Sandbox lähettää kerätyn datan eteenpäin analysoitavaksi. Joillakin laitevalmistajilla data lähetetään erilliseen pilveen analysoitavaksi. Analyysissä dataa verrataan olemassa olevaan tietokantaan. Tiedosto tai sovellus estetään ja tuhotaan, jos sen käytös todetaan haitalliseksi tai erillinen analysointi tunnistaa sen haittaohjelmaksi. Sandboxin vahvuus on, että se voi estää ennestään tuntemattomia hyökkäyksiä. Kenenkään valmistajan tietokanta ei voi pysyä täysin ajan tasalla uusien ja tuntemattomien uhkien torjumiseksi. Sandboxin heikkoutena on, ettei se välttämättä toimi täydellisesti esimerkiksi kannettavilla laitteilla. Käyttäjät voivat mahdollisesti asentaa sovelluksia laitteisiinsa hallitun verkon ulkopuolella. Vaihtoehtoisesti myös vertaisverkkoyhteydet, kuten Skype ja BitTorrent, voivat mahdollisesti ohittaa sandbox-tarkastelun. Myös uudet liikennettä salaavat protokollat, kuten IPv6, voivat läpäistä palomuurin ilman tarkastelua. Sandboxing ei ole muutenkaan täysin varma vaihtoehto, koska tarkastelu on lyhytaikaista, jolloin haitallista toimintaa ei välttämättä ehdi tapahtumaan. Varma tarkastelutulos voi vaatia päivistä viikkoihin kestävän karanteenin. (Webroot Inc. 2014, 6.)



KUVIO 4. Sandboxin toiminta uhkien torjunnan välineenä (Webroot Inc. 2014, 6)

Uhkien torjuntaa voidaan tehdä myös ennakoivasti. Tällaisessa menettelyssä palomuuri hakee säännöllisesti tietokantaansa päivityksiä riskeistä. Riskit yleensä pisteytetään niiden uhkatason mukaan. Ennakoiva uhkien torjunta voi muun muassa pisteyttää IP-osoitteita, domaineja ja mobiilisovelluksia. Esimerkiksi IP-osoitteiden pisteytyksissä ison painoarvon luo osoitteen ikä ja suosio. (Webroot Inc. 2014, 6-7.)

3.2.2 Tunkeutujanestojärjestelmä

Tunkeutujanestojärjestelmä (Instrusion Prevention System, IPS) on ohjelmisto, jonka tehtävänä on tunnistaa verkkoon tapahtuvia hyökkäysyrityksiä ja tarvittaessa estää niitä. Tunkeutujanestojärjestelmän toiminta perustuu erilaisien tunnistimien käyttöön. Tunnistimet monitoroivat erilaisia osa-alueita, joissa hyökkäykset voivat näkyä. Tunkeutujanestojärjestelmä voi tunnistaa hyökkäyksen ennestään tunnetusta haitallisesta

käyttäytymisestä tietokantaansa vertaamalla tai vastaavasti tunnistaa normaalista poikkeavaa käytöstä. (Gregg 2014.)

3.2.3 SSL- ja TLS-salauksen purku

Jotta sovellustunnistus ja sisällöntunnistus toimisivat moitteettomasti, on sen päästävä tarkastelemaan SSL- ja TSL-suojattujen pakettien sisältöä. Seuraavan sukupolven palomuurit tarjoavat työkalun SSL- ja TLS-salauksien purkuun.

SSL (Secure Sockets Layer) on yksi yleisimmistä salausprotokollista. Palo Alto Networksin tutkimuksen mukaan vuonna 2014 jopa 26 % kaikista sovelluksista käytti SSL:ää jossakin muodossa. 85 sovellusta 356:sta eivät koskaan käyttäneet SSL-oletusporttia 443. Sovellukset käyttivät joko porttia TCP/80 tai muuta vaihtoehtoa. Suurin osa näistä sovelluksista myös vaihtoi porttia ajoittain. Tämä osoittaa hyvin, että porttikohtaiset palomuurisäännöt eivät ole enää täysin luotettavia. SSL-suojattu liikenne kasvaa jatkuvasti, mikä luo entistä enemmän riskejä. Esimerkiksi Google priorisoi SSL:ää hakutuloksissaan. SSL-suojauksen takana toimivat sosiaalisen median palvelut ovat myös optimaalisia haittaohjelmien levittämiseen. (Humphreys & Robertson 2014.)

SSL-salauksen purku voidaan tehdä sekä sisään että ulos tulevasta liikenteestä. Useimmissa ympäristöissä ei ole kuitenkaan järkevää purkaa kaikkia salauksia, koska se vaatii palomuurilta paljon resursseja, eikä siitä saada merkittävää hyötyä. Salauksen purkamiselle voidaan luoda sääntöjä esimerkiksi alueen, käyttäjän, ryhmän, lähde- ja kohdeosoitteen tai URL-kategorian mukaan. Esimerkiksi joissakin tilanteissa riskiryhmään kuuluvien henkilöiden liikenne voitaisiin aina purkaa. Salauksen purun jälkeen paketti voidaan toimittaa sisällöntunnistukseen, jossa sille voidaan tehdä halutut toimenpiteet. (Humphreys & Robertson 2014.) SSL-liikenteen purkaminen on myös herättänyt keskustelua työntekijöiden yksityisyydestä, koska SSL-liikenteen purku toimii käytännössä samalla tavalla kuin man-in-the-middle -hyökkäys. Esimerkiksi Palo Alto Networksin laitteissa käytetään salauksen purkamiseen sertifikaatin kopiointi -tekniikkaa. (Messmer 2012.)

3.3 Virtuaalisovellukset

Monet laitevalmistajat tarjoavat mahdollisuuden asentaa virtuaalisia sovelluksia palomuureihinsa. Esimerkiksi Palo Alto Networks tarjoaa osaan laitteistaan mahdollisuuden asentaa virtuaalisia palomuureja. Virtuaaliset palomuurit tarjoavat mahdollisuuden luoda sisäverkkoon rakenteen, jossa on vain yksi fyysinen laitepalomuuri ja monta loogista virtuaalista muuria. Virtuaaliset muurit ovat topologiassa erillään

toisistaan ja niihin voidaan määritellä erilaiset säännöt. Virtuaalimuurien käyttö on tehokasta, koska niitä voidaan luoda ja muokata nopeasti. (Palo Alto Networks 2018e.) Se mahdollistaa esimerkiksi verkon hajauttamisen useaan osaan, jolloin esimerkiksi samassa rakennuksessa työskentelevät yritykset voisivat käyttää yhtä samaa fyysistä palomuuria. Ylläpitäjille voitaisiin tässä tapauksessa antaa oikeudet hallinnoida vain oman toimialansa virtuaalista muuria.

3.4 Käyttäjätunnistus

Seuraavan sukupolven palomuurien hyödyllisimpiä ominaisuuksia on käyttäjän identiteetin tunnistus. Internetin käyttö on muuttunut kannettavien laitteiden myötä sellaiseksi, että pelkillä IP-osoitteilla täysin toimivien ja turvallisten palomuurisääntöjen tekeminen on lähes mahdotonta. Identiteetin tunnistuksen avulla voidaan todentaa käyttäjä aina samaksi riippumatta siitä, onko hän millä tavalla yhteydessä toimialansa verkkoon. Hän saa silti aina tälle määritetyt omat palomuurisäännöt. Tyypillisesti henkilö voi liittyä esimerkiksi työpaikkansa verkkoon langallisesti, langattomasti tai VPN:n avulla. Identiteetin tunnistus toimii yleensä jonkin kolmannen osapuolen käyttäjähallintapalvelun kanssa. Tyypillisesti käyttäjätiedot saadaan toimialueen Active Directorystä tai vaikkapa RADIUS-palvelimelta. Identiteetin tunnistus auttaa antamaan käyttäjälle samat palomuurisäännöt riippumatta hänen laitteensa IP-osoitteesta. Sääntöjä voidaan hallita joko yksilö- tai ryhmätasolla, jolloin ympäristöstä voidaan saada mahdollisimman turvallinen. Tämä mahdollistaa tiettyjen sovelluksien sallimisen vain niitä tarvitseville henkilöille. Esimerkiksi tämä mahdollistaa sen, että voitaisiin määritellä sääntö, jossa vain IT-osaston työntekijöillä on oikeus SSH-, Telnet- ja FTP-yhteyksiin, kun ne kohdistuvat oletusportteihin. (Palo Alto Networks 2016b.)

Laitevalmistajat tarjoavat erilaisia tapoja identiteetin tunnistuksen toteuttamiseen ja mahdollisuuksia sen hyödyntämiseen. Monitorointi auttaa ymmärtämään verkonkäyttöä henkilö- ja ryhmätasolla, jonka avulla voidaan luoda sääntöjä parantamaan tietoturvaa.

3.5 Muut ominaisuudet

Seuraavan sukupolven palomuureja voidaan myös virtualisoida. Osa palomuureista voidaan virtualisoida esimerkiksi Citrixiin, Hyper-V:hen tai Microsoftin Azure-pilvipalveluun. Virtualisoidun palomuurin haittana voi olla, ettei siinä ole täysin kaikkia samoja ominaisuuksia, mitä erillisessä palomuurilaitteessa on. Esimerkiksi Ciscon virtualisoidussa seuraavan sukupolven palomuurissa ei ole VPN-tukea. (Cisco Systems 2018b.)

Seuraavan sukupolven palomuureissa voi olla myös yksittäisiä laitevalmistajan tarjoamia ominaisuuksia, joita kilpailijat eivät tarjoa. Tällaisia ominaisuuksia voivat olla esimerkiksi palomuurin synkronointi muiden verkkolaitteiden kanssa, kuten reitittimien, kytkimien ja langattomien tukiasemien kanssa. Tällaiset ominaisuudet ovat usein rajattu pelkästään laitevalmistajan omiin laitteisiin, eivätkä ominaisuudet toimi välttämättä kilpailijoiden laitteiden kanssa.

4 PALOMUURIN VALINTA

Työosuus alkoi eri valmistajien palomuureja vertailemalla. Ennestään oli tutustuttu Palo Alto Networksin palomuureihin ja löydetty potentiaaliseksi vaihtoehdoksi malli PA-5220. Tarkoitus oli tutustua PA-5220:n ominaisuuksiin ja vertailla sitä muutaman muun laitevalmistajan laitteisiin. Tarkoituksena oli löytää ominaisuuksiltaan samanlainen tuote. Vaihtoehtoja tutkittiin kolmen muun laitevalmistajan laitteista, joihin kuuluivat Cisco, Sophos ja Check Point. Potentiaalisten laitteiden ominaisuudet kirjattiin ylös ja niille etsittiin listahinnat. Näiden tietojen pohjalta palomuurit kilpailutettiin eri toimittajien väliltä.

Vertailussa otettiin huomioon seuraavat tekijät:

- palomuurin läpäisykyky
- läpäisykyky sovellukset päällä
- sovellustason tunnistus
- käyttäjätunnistus
- hyökkäyksentunnistus
- hyökkäykseneston läpäisykyky
- nollapäivähyökkäyssuoja
- virustorjunta
- liitäntöjen lukumäärä (max) ja niiden tyypit
- VPN/SSL-VPN läpäisykyky
- virtuaalisovellusten lukumäärä
- yhteyksien lukumäärä (max)
- yhteydet/sekunti
- lisenssit ja listahinta.

Tutkimuksen alkuvaiheessa todettiin, että kaikki vertailuun valitut laitteet sisälsivät tärkeimmät seuraavan sukupolven palomuurien ominaisuudet, joita olivat muun muassa sovellustunnistus, käyttäjätunnistus, hyökkäyksenesto ja virustorjunta. Tämän vuoksi

työssä perehdyttiin myös laitevalmistajien markkinointimateriaaleissa painotettuihin ominaisuuksiin ja eroavaisuuksiin kilpailijoihinsa nähden.

4.1 Palo Alto PA-5220

Palo Alto PA-5220 on amerikkalaisen Palo Alto Networksin seuraavan sukupolven palomuuri. Se on suuryrityksien käyttöön suunniteltu laite, joka tarjoaa kaikki olennaisimmat seuraavan sukupolven palomuurin ominaisuudet. Se tarjoaa jopa 18 Gb/s läpäisykyvyn sovellustunnistus päällä sekä jopa neljän miljoonan yhtäaikaisen istuntojen määrän. Palo Alto PA-5220 -palomuurin suorituskyvyllisiä ominaisuuksia on esitetty taulukossa 1.

Taulukko 1. Laitteen PA-5220 suorituskyvylliset ominaisuudet (Palo Alto Networks 2018d)

Ominaisuus	Kapasiteetti
Palomuurin läpäisykyky (App-ID päällä)	18 Gb/s
Uhkien torjunnan läpäisykyky	8 Gb/s
IPsec VPN läpäisykyky	8 Gb/s
Istuntojen maksimi määrä	4 000 000
Uudet istunnot sekunnissa	171 000
Virtuaalijärjestelmien lukumäärä (valmiit/maksimi)	10 / 20*
*Enimmäismäärän saavuttaminen vaatii erikseen ostetun lisenssin	

4.1.1 Toimintatavat

Palo Alto PA-5220 tarjoaa hyvät liitäntämahdollisuudet, mikä mahdollistaa sen käytön erilaisissa ympäristöissä erilaisilla toimintatavoilla. PA-5220 voidaan asentaa verkkoon neljällä päätavalla: Tap-, Virtual Wire-, Layer 2- ja Layer 3 -tiloissa.

Tap-tilassa PA-5220 monitoroi jo käytössä olevan palomuurin sääntöjä ja turvallisuusuhkia. Se monitoroi verkon liikennettä käyttämällä porttien peilaustekniikkaa. Se antaa mahdollisuuden nähdä verkossa ilmenevät sovellukset, haavoittuvuudet ja uhkat. Tap-tila on hyvä tapa aloittaa oman verkkonsa kartoitus, koska se ei vaadi muutoksia verkon rakenteeseen. Tap-tilan heikkous on, ettei se voi estää liikennettä. Sen tarkoitus on vain raportoida siitä. (Infinity Technology Services 2018.)

Virtual Wire -tilassa palomuuri toimii ikään kuin näkymättömänä laitteena verkossa. Tämä ominaisuus toimii, kun palomuurin kaksi porttia sidotaan (binding) yhteen. Virtual Wire -tilaa tulisi käyttää vain, jos halutaan yhdistää palomuuri saumattomasti topologiaan, eikä yhteen sidottujen porttien tarvitse tehdä aliverkkojen kytkentää tai reititystä. Virtual Wire

yksinkertaistaa palomuurin asentamista ja konfigurointia, koska sen voi liittää helposti valmiina olevaan topologiaan ilman MAC- tai IP-osoitteiden määritystä, verkon uudistamista tai ympärillä olevien verkkolaitteiden asetusten uudelleenmäärittelyä. (Infinity Technology Services 2018.)

Layer 2 -tilassa palomuuri tarjoaa mahdollisuuden kytkeä kaksi tai useamman verkon yhteen. Se käyttäytyy kuin OSI-mallin tason 3 kytkin. Palomuurin porteille määritetään VLAN:t. (Infinity Technology Services 2018.)

Layer 3 -tilassa palomuuri reitittää liikennettä useiden porttien välillä. Palomuurin liitännöille määritetään IP-osoitteet ja palomuuriin konfiguroidaan virtuaaliset reitittimet reitittämään liikennettä. Layer 3 -tilaa käytetään, kun reitittäminen on välttämätöntä. (Infinity Technology Services 2018.)

Palo Alto tarjoaa suorituskykyisen tarkastelun heidän patentoidulla Single-Pass-tekniikalla. Nimensä mukaisesti tällä tavalla toteutettu tekniikka luokittelee ja kontrolloi liikennettä vain kerran yhtä pakettia kohden. Single-Pass-teknologia tarkastelee datavirtaa yksittäisten tiedostojen sijaan, jolloin tarkastelun tuoma viive on huomattavasti pienempi. Single-Pass-arkkitehtuuriin sisältyy Palo Alton patentoidut App-ID-, User-ID- ja Content-ID-teknologiat sekä erillinen Policy Engine. Nämä teknologiat mahdollistavat sovellus-, käyttäjä- ja sisältötunnistuksen, joiden avulla paketit joko sallitaan tai estetään. (Palo Alto Networks 2016a.)

App-ID on Palo Alton tekniikka sovellustunnistukseen. Se antaa mahdollisuuden nähdä sovellukset verkossa, jolloin palomuuri voi oppia niiden toimintatapoja, käyttäytymistä, ominaisuuksia ja mahdollisia riskejä. Se hyödyntää useita tekniikoita identifioimiseen, joita ovat esimerkiksi sovelluksien allekirjoitukset, SSL-salauksen purku sekä protokollien avaus. Se antaa myös mahdollisuuden käyttäjän itse nähdä tietoja sovelluksista verkossa. (Palo Alto Networks 2018b.)

User-ID on Palo Alton käyttäjätunnistusteknologia. User-ID mahdollistaa käyttäjien tunnistuksen käyttäen erilaisia tekniikoita kuten liityntätapojen ja käyttöjärjestelmien avulla. Tuettuja käyttöjärjestelmiä ovat Microsoft Windows, Apple iOS, Mac OS, Android ja Linux. User-ID antaa järjestelmänvalvojalle tarkemman kuvan verkon käytöstä. User-ID:n avulla voidaan nähdä, ketkä käyttäjät käyttävät mitäkin sovelluksia. (Palo Alto Networks 2016b.)

4.1.2 Lisenssit ja listahinnat

Palo Alton lisenssit jakautuvat useisiin eri osa-alueisiin, joita voidaan ostaa erikseen. Näitä osa-alueita ovat uhkientorjunta, salauksen purkamisen peilaus, URL-suodatus, Virtuaalijärjestelmät, WildFire, GlobalProtect ja AutoFocus.

Taulukko 2. Palo Alton seuraavan sukupolven palomuurien lisenssejä (Palo Alto Networks 2018a)

Lisenssi	Sisältö
Threat Prevention	Antivirus, anti-spyware, haavoittuvuussuoja
Decryption Mirroring	Palomuuri purkaa ja kopioi liikenteen analysoitavaksi.
URL Filtering	Antaa mahdollisuuden luoda sääntöjä tarkkailemaan web-liikennettä dynaamisten URL-kategorioiden avulla. Voidaan käyttää joko PAN-DB tai BrightCloud-tietokannan kanssa.
Virtual Systems	Antaa mahdollisuuden asentaa useampia virtuaalijärjestelmiä palomuuriin.
WildFire	Laajempi suoja WildFireen (joka sisältyy Threat Prevention –lisenssiin). Allekirjoituksien päivitykset, kehittyneiden tiedostotyyppien välittäminen ja mahdollisuus ladata tiedostoja suojaan WildFire API:iin.
GlobalProtect	Mahdollisuus laaja-alaisempaan VPN:ään. GlobalProtect voidaan määritellä käyttöön ilman lisenssiä, mutta lisenssin ostaessa saadaan käyttöön käyttäjätietoprofiili (Host Information Profile, HIP), jolla voidaan valvoa tarkemmin dataa.
AutoFocus	Tarjoaa graafisen analyysin palomuurin liikennelogeista ja tunnistaa potentiaaliset riskit sisäverkosta.

Palo Alto PA-5220 -laitteen listahintoja voidaan tulkita taulukosta 3. Laite ilman älykkäitä ominaisuuksia maksaa noin $ 61,952. Älykkäiden ominaisuuksien lisenssit ovat keskenään saman hintaisia lukuun ottamatta URL-suodatusta. Palo Alton lisenssejä voidaan ostaa yhdeksi, kolmeksi tai viideksi vuodeksi kerrallaan. Lisenssien uusiminen on halvempaa kuin ensimmäisellä kerralla ostaminen.

Taulukko 3. Palo Alto PA-5220 -laitteen listahintoja (CDW 2018)

Laitteen nimi	PA-5220	Voimassaoloaika
Laitteen listahinta	$ 61,951.99	-
WildFire	$ 21,648.99	3 vuotta
Threat Prevention	$ 21,648.99	3 vuotta
URL Filtering	$ 28,084.99	3 vuotta
GlobalProtect	$ 21,648.99	3 vuotta
Lisävirtuaalimuurit (10 kpl)	$ 21,941.99	-

4.2 Cisco Firepower

Firepower on amerikkalaisen verkkolaiteita valmistavan Cisco Systemsin seuraavan sukupolven palomuurisarja. Ciscolla on laaja valikoima erilaisia palomuureja erilaisiin toimintaympäristöihin. Firepower-sarjan lisäksi Cisco tarjoaa myös pienenpiin ympäristöihin ASA-palomuurisarjaa, jossa on myös seuraavan sukupolven palomuurin ominaisuudet.

Firepowerin 4100-sarjan laitteet todettiin käyttötarkoitukseen sopivilta. Tästä sarjasta valikoitui vertailuun kaksi laitetta: Firepower 4110 ja 4120. Firepower-sarjan laitteet tarjoavat perinteisten seuraavan sukupolven palomuurien ominaisuuksien lisäksi myös muun muassa seuraavan sukupolven tunkeutumisjärjestelmän (NGIPS) ja kehittyneen haittaohjelmasuojan (Advanced Malware Protection, AMP). (Cisco Systems 2018a.) Ciscon seuraavan sukupolven palomuurit tukevat myös avoimeen lähdekoodiin perustuvaa kolmannen osapuolen maineikasta tunkeutujanhavaitsemisjärjestelmä Snortia ja siihen Ciscon kehittämää lisäosaa OpenAppID:tä. (Cisco Systems 2018b.) Cisco Firepower 4110 ja 4120 –laitteiden suorituskyvyllisiä ominaisuuksia on esitetty taulukossa 4.

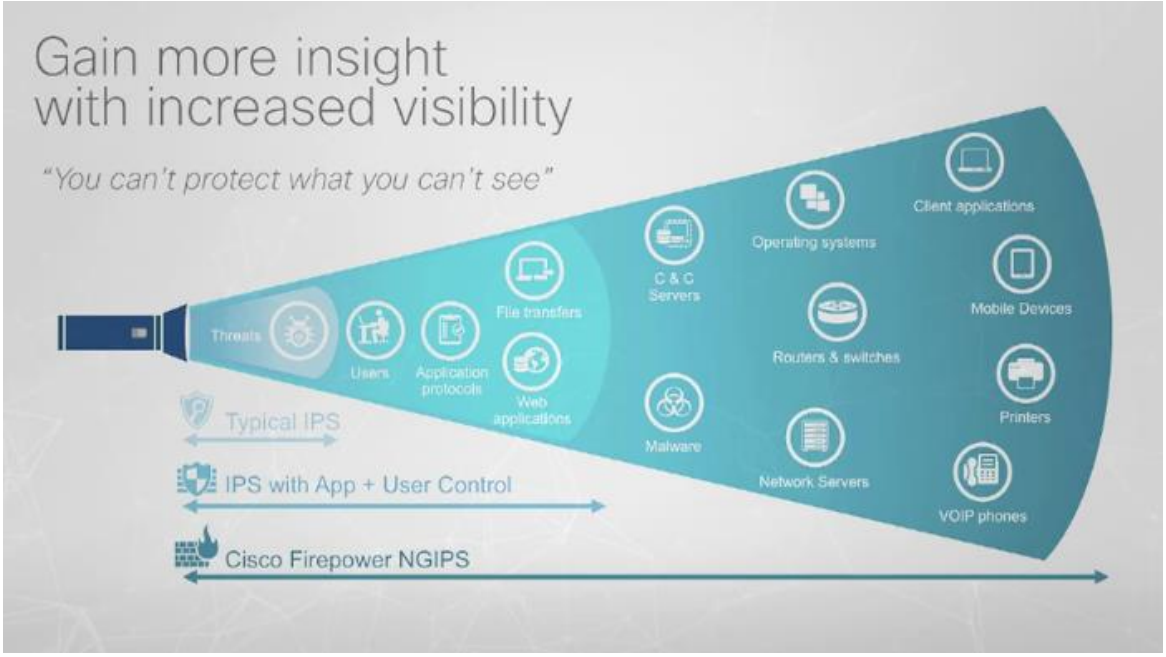
Taulukko 4. Cisco Firepower 4110 ja 4120 -laitteiden suorituskyvyllisiä ominaisuuksia (Cisco Systems 2018b)

Ominaisuus	Firepower 4110	Firepower 4120
Palomuurin läpäisykyky	12 Gb/s	20 Gb/s

sovellustunnistus päällä		
Palomuurin läpäisykyky sovellustunnistus ja tunkeutumisenestojärjestelmä päällä	10 Gb/s	15 Gb/s
IPSec VPN läpäisykyky	6 Gb/s	10 Gb/s
Istuntojen maksimimäärä	9 000 000	15 000 000
Uudet istunnot sekunnissa	68 000	120 000

4.2.1 Toimintatavat

NGIPS (Next-Generation Intrusion Prevention System) on Ciscon vastine perinteiselle tunkeutumisenestojärjestelmälle. NGIPS mahdollistaa näkemään uhkia, joita perinteinen tunkeutumisenestojärjestelmä ei pysty havaitsemaan. Seuraavan sukupolven palomuurit yhdistävät usein sovellus- ja käyttäjäkontrolloinnin tunkeutumisenestojärjestelmään, mutta NGIPS vie sen sitäkin pidemmälle. NGIPS näkee muun muassa sisäverkossa toimivat käyttöjärjestelmät, mobiililaitteet, tulostimet, reitittimet ja kytkimet. NGIPS pystyy tarkastelemaan laitteiden tilaa ilman erillistä päätelaitteelle asennettavaa agent-ohjelmistoa. NGIPS:n näkemiä kohteita on esitetty kuviossa 5. (Cisco Systems 2018e)



Kuvio 5. Ciscon hahmotelma NGIPS:n ominaisuuksista. (Cisco Systems 2018e)

Cisco Firepowerin ominaisuuksiin kuuluu tarkkailla pakettia vielä senkin jälkeen, kun paketti on päässyt palomuurista läpi sisäverkkoon. Tämä antaa mahdollisuuden havaita haitalliset kohteet, jotka näyttävät aluksi puhtailta, mutta alkavat myöhemmin käyttäytyä haitallisesti.

Sandboxing on toteutettu Ciscon seuraavan sukupolven palomuureissa pilvipohjaisella ratkaisulla. Cisco kutsuu heidän sandbox-tekniikkaansa nimellä Cisco Threat Grid, jossa käytetään Ciscon kehittynyttä uhkasuojaa (AMP). AMP:n tietokanta on valtava. Ciscon uhkantunnistusyksikössä Talosissa analysoidaan joka päivä useita terabittejä dataa, jotka sisältävät miljoonia haittaohjelmanäytteitä. Tämä tieto sisällytetään AMP:iin. AMP käsittelee saadut tiedot, joita se käyttää tietokantansa parantamiseen. Tällä tavoin voidaan ennakoivasti estää tunnettuja ja tulevia uhkia. (Cisco Systems 2018a.)

4.2.2 Lisenssit ja listahinnat

Cisco Firepower -laitteet lisensoidaan Ciscon smart licensing -tekniikalla. Smart licensing mahdollistaa lisenssien hallinnan keskitetysti. Smart lisenssit eivät ole sidottuja tiettyyn sarjanumeroon tai laitteen aktivointiavaimeen (Product Activation Key, PAK). Smart licencing antaa ylläpitäjälle mahdollisuuden arvioida lisenssin käyttöä ja tarpeita yhdellä silmäyksellä. (Cisco Systems 2018d.)

Firepower 4100-sarjan laitepalomuureihin on saatavilla viisi erilaista lisenssiä, jotka ovat base, threat, malware, URL filtering ja Remote Access VPN. Base-lisenssi on palomuurissa automaattisesti, eikä se sisällä älykkäitä ominaisuuksia. Se on myös voimassa ikuisesti. Threat-lisenssi sisältää tunkeilijanestojärjestelmän, tiedostohallinnan sekä Ciscon Security Intelligence -suodatuksen. Malware-lisenssi sisältää Ciscon kehittyneen haittaohjelmasuojan (Cisco Advenced Malware Protection, AMP) tiedostojen tarkasteluun. URL Filtering -lisenssi sisältää nimensä mukaisesti työkalut URL-suodatukseen, jotka voidaan tehdä kategorian tai URL:n maineen perusteella. Yksittäisiä URL:ja voidaan kuitenkin suodattaa ilman lisenssiä. RA VPN -lisenssi sisältää mahdollisuudet käyttää Ciscon AnyConnect VPN:ää. Lisenssejä voidaan ostaa erilaisina ohjelmistopaketteina, joka sisältää tietyt ominaisuudet. Ohjelmistopaketit ovat T (Threat), TM (Threat + Malware), TMC (Threat + Malware + URL) ja AMP. Lisenssit on esitetty myös taulukossa 5. (Cisco Systems 2018d.)

Taulukko 5. Cisco Firepower 4100 -sarjaan saatavat lisenssit (Cisco Systems 2018d)

Lisenssi	Tilaus	Sisältö
Base	-	Käyttäjä- ja sovellushallinta, reititys ja kytkentä, NAT
Threat	T	Tunkeilijanesto, tiedostohallinta, älykäs suodatus
Malware	TM, TMC, AMP	AMP for Networks, AMP Threat Grid
URL filtering	TC, TCM, AMP	URL-suodatus maineen ja kategorian mukaan
Remote Access VPN	Riippuu lisenssistä	AnyConnect VPN (erilaisia vaihtoehtoja)

Cisco Firepower -laitteiden listahintoja voidaan tarkastella taulukosta 6. Cisco Firepower -laitteisiin voidaan ostaa lisenssejä yhdeksi, kolmeksi tai viideksi vuodeksi kerrallaan. Jälleenmyyjät tarjoavat myös erilaisia paketteja, joihin sisältyy useampia lisenssejä.

Taulukko 6. Cisco Firepower 4410 ja 4120 -laitteiden ja lisenssien listahintoja (IT Price 2018a) (IT Price 2018b)

	Firepower 4410	Firepower 4120	Voimassaoloaika
Laitteen listahinta	$ 89,995	$ 149,995	-
Threat Protection	$ 54,000	$ 90,000	3 vuotta
Malware Protection	$ 43,200	$ 72,000	3 vuotta
URL filtering	$ 43,200	$ 72,000	3 vuotta

4.3 Check Point

Check Point on israelilainen monikansallinen yritys, joka tuottaa tietoturvaohjelmistoja ja laitteita. Check Point tarjoaa useita seuraavan sukupolven palomuureja eri kokoisiin ympäristöihin. Vertailuun valittiin kaksi laitetta Enterprise 15000 -sarjasta, jotka olivat 15400 ja 15600. Laitteiden 15400 ja 15600 -laitteiden suorituskyvyllisiä ominaisuuksia ideaalisessa ja todenmukaisessa ympäristössä on eritelty taulukoissa 7 ja 8. Check Point oli vertailun ainoa laitevalmistaja, joka eritteli palomuurin suorituskyvylliset ominaisuudet ideaaliympäristön ja todenmukaisen ympäristön välillä.

Taulukko 7. Check Point 15400 ja 15600 -palomuurien suorituskyvyllisiä ominaisuuksia ideaaliympäristössä (Check Point 2017, 2)

Laite	15400	15600
Palomuurin läpäisykyky	58 Gb/s	76 Gb/s
Palomuurin läpäisykyky sovellukset päällä	12,5 Gb/s	17 Gb/s
IPS läpäisykyky	14 Gb/s	18 Gb/s
Uhkien torjunnan läpäisykyky	7 Gb/s	13,11 Gb/s
VPN läpäisykyky	10,8 Gb/s	15,8 Gb/s
Istuntojen maksimimäärä	3,2 / 25 miljoonaa*	6,5 / 25 miljoonaa*
Uudet istunnot sekunnissa	185 000	185 000
*Enimmäismäärän saavuttaminen valmiiksi asennetulla / maksimi muistilla		

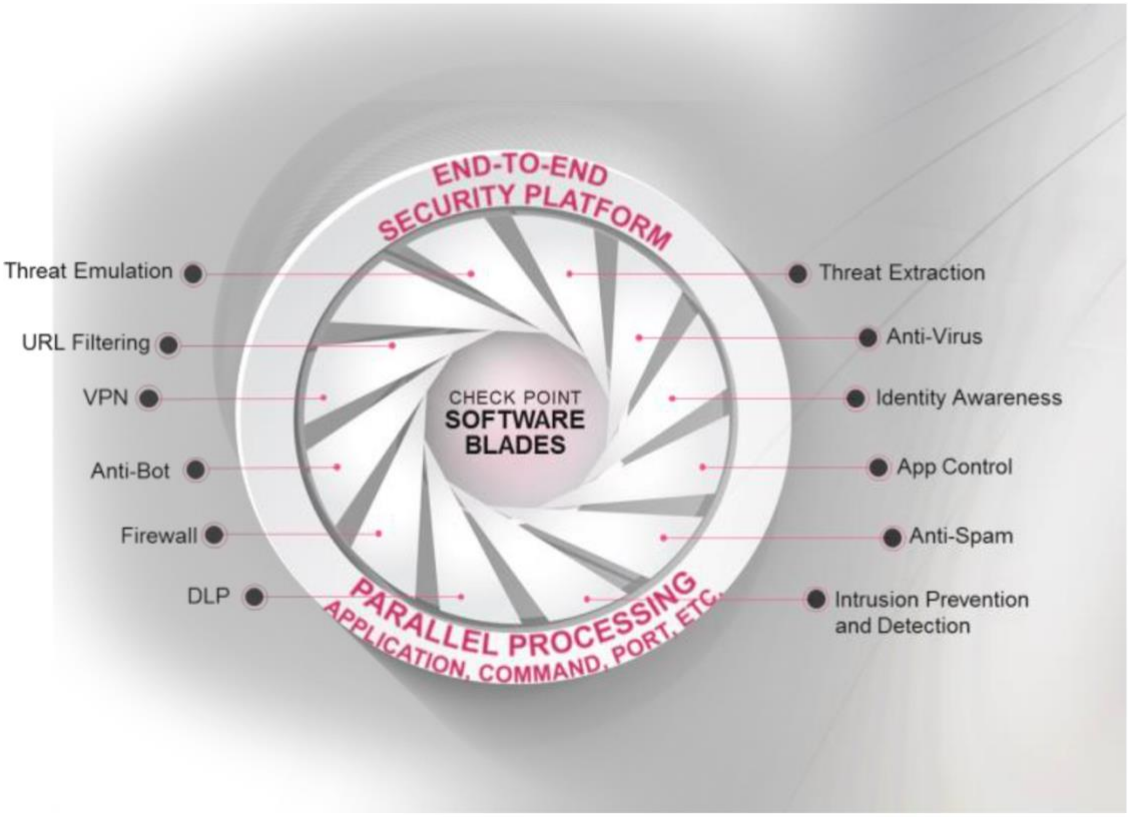
Taulukko 8. Check Point 15400 ja 15600 -palomuurien suorituskyvyllisiä ominaisuuksia todenmukaisessa ympäristössä (Check Point 2017, 2)

Laite	15400	15600
Palomuurin läpäisykyky	30 Gb/s	30 Gb/s
Palomuurin läpäisykyky sovellukset päällä	3 Gb/s	5,2 Gb/s

IPS läpäisykyky	4,5 Gb/s	8 Gb/s
Uhkien torjunnan läpäisykyky	1,695 Gb/s	3 Gb/s

4.3.1 Toimintatavat

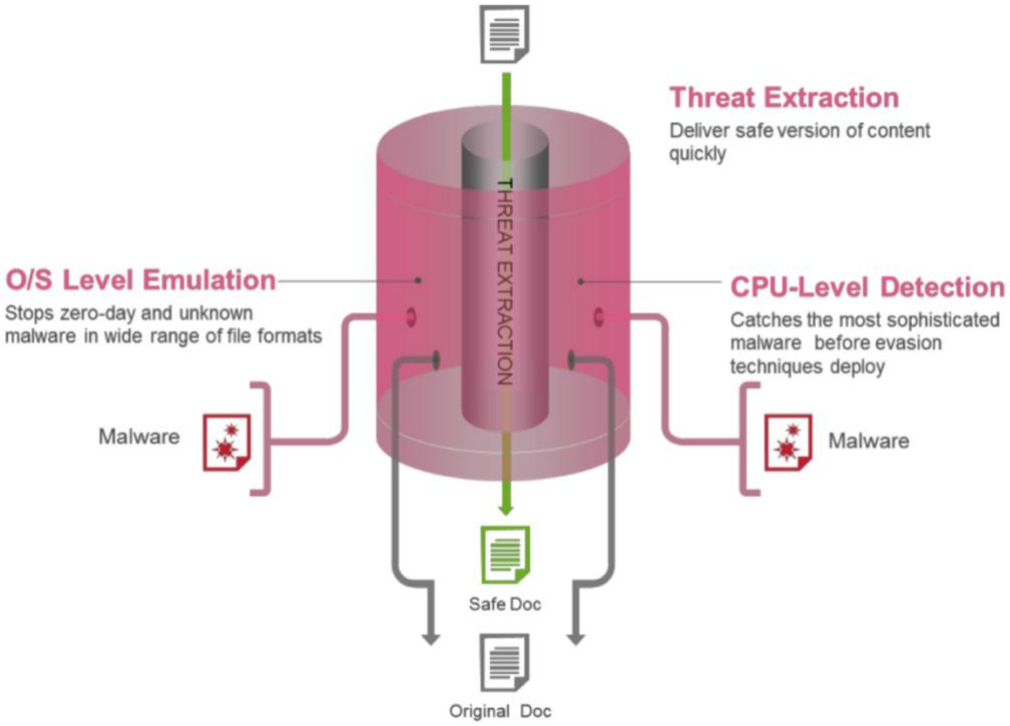
Check Point kutsuu erilaisia sovelluksiaan Software Bladeiksi, jotka on esitetty kuviossa 6. Kuten kuviosta 6 voidaan todeta, myös Check Pointin seuraavan sukupolven palomuureista löytyvät tärkeimmät ominaisuudet tietoturvallisen ympäristön takaamiseksi.



Kuvio 6. Check Point Software Bladet (Check Point 2018c, 3)

Anti-Bot-ohjelmisto estää nimensä mukaisesti bot-tyyppisiä haittaohjelmia, jotka antavat hyökkääjille mahdollisuuden etähallita tietokoneita ja tehdä laittomia toimia, kuten varastaa dataa ja levittää roskapostia sekä haittaohjelmia. Anti-Bot-ohjelmisto tunnistaa bot-haittaohjelmilla saastuneet koneet ja estää bottia tekemästä vahinkoa estämällä sen liikennettä. Anti-Bot-ohjelmisto päivittyy automaattisesti ThreatCloudista. ThreatCloud analysoi joka päivä yli 75 miljoonaa osoitetta bottien löytämiseksi. (Check Point 2018a.)

SandBlast on Check Pointin vastine sandboxing-tekniikalle, jota havainnollistetaan kuvio 7. SandBlast on jaettu kahteen osaan, jotka ovat Threat Emulation ja Threat Extraction. Threat Emulation suorittaa prosessoritason tarkastelun, jonka avulla voidaan estää suurin osa hyökkäyksistä ennen kuin haittaohjelmalla on mahdollisuutta edes aloittaa toiminta. Tällä tavalla voidaan myös estää haittaohjelman kiertämästä tai huijaamasta tarkastelua. Threat Extraction täydentää tätä ratkaisua välittämällä turvallista sisältöä nopeasti joko haittaohjelmista puhdistetulla tai vastaavasti uudelleenrakennetulla versiolla. Tällä tavalla toteutettuna sandbox ei aiheuta viivettä. (Check Point 2016, 1-2)



KUVIO 7. Check Pointin hahmotelma SandBlastin toiminnasta. (Check Point 2016, 2)

Check Pointin palomuureissa on asennettuna GAiA-käyttöjärjestelmä. GAiA on sisältää tuen Software Bladeille, yhdyskäytäville ja turvallisuudenhallintatuotteille. GAiA-käyttöjärjestelmää voidaan käyttää joko komentoriviltä tai web-käyttöliittymästä. (Check Point 2018c, 4.)

4.3.2 Lisenssit ja listahinnat

Check Pointin seuraavan sukupolven palomuurien lisensointi on yksinkertaisin kilpailijoihinsa nähden. Check Point on jakanut lisenssit kahteen ohjelmistopaketteihin. Ensimmäisen ohjelmistopaketin nimi on Next Generation Threat Prevention (NGTP), joka sisältää monikerroksisen suojauksen tunnetuilta, allekirjoituksiin perustuvilta uhilta käyttämällä antivirusta, antibottia, IPS:ää, App Controlia, URL-suodatusta sekä

käyttäjätunnistusta. Toinen ohjelmistopaketti on Next Generation Threat Prevention & Sandblast (NGTX), joka sisältää ensimmäisen paketin ominaisuuksien lisäksi Check Pointin Sandblast-sandboxin nollapäivähaavoittuvuuksia vastaan. (Check Point 2018d.)

Check Pointin listahintoja on eritelty taulukossa 9. Check Pointin palomuureja voidaan ostaa kolmella erilaisella komponenttikokoonpanolla. Palomuurin voi valita joko Base-, HPP- tai Max-kokoonpanolla, jossa vaihtuvat esimerkiksi porttien, keskusmuistin ja kovalevyjen määrä. Laitteen 15400 kokoonpanojen eroja on eritelty taulukossa 10. Mallin 15600 ainoa ero oli Base-kokoonpanon ”HDD or SSD” –kohdan lukumäärä, joka oli kaksi. Palomuurin voi ostaa pakettina, johon sisältyy NGTX-lisenssi. (Check Point 2018d.)

Taulukko 9. Check Point 15400 ja 15600 -laitteiden listahintoja (Check Firewalls 2018a) (Check Firewalls 2018b)

Laitteen nimi	15400	15600	Voimassaoloaika
Laite (Base)	$ 63,000	$ 79,000	-
Laite (Base) + NGTX	$ 71,700	$ 89,800	1 vuosi
Laite (HPP)	$ 77,500	$ 91,000	-
Laite (HPP) + NGTX	$ 86,500	$ 101,800	1 vuosi

Taulukko 10. Check Point 15400-palomuurin kokoonpanovaihtoehdot (Check Point 2018b, 2)

	Base	HPP	Max
1 GbE ports (Copper)	10	10	26
10 GbE ports (Fiber)	2	6	12
Transceivers (SR)	2	6	12
40 GbE ports (Fiber)	0	0	4
100/25 GbE ports (Fiber)	0	0	4
RAM	8GB	24GB	64GB
HDD or SSD	1	2	2
AC or DC Power Units	2	2	2
Lights Out Management	Included	Included	Included

4.4 Sophos

Sophos on britannialainen tietoturvayhtiö, jonka tuotteisiin kuuluvat erilaiset tietoturvaohjelmistot ja -laitteet. Sophosin vastaus seuraavan sukupolven

palomuurikilpailuun on heidän XG-sarjansa laitteet. Vertailuun otettiin mukaan laitteet XG 550 ja XG 650. Suorituskyvyltään XG-sarjan laitteet ovat hyvin kilpailukykyisiä. Esimerkiksi XG 650 lupaa liikenteen läpäisykyvyn nopeudeksi sovellukset päällä 10 Gb/s sekä jopa 30 000 000 yhtäaikaista istuntoa.

Taulukko 11. Sophosin XG 550 ja 650 -palomuurien suorituskyvyllisiä ominaisuuksia (Sophos 2018)

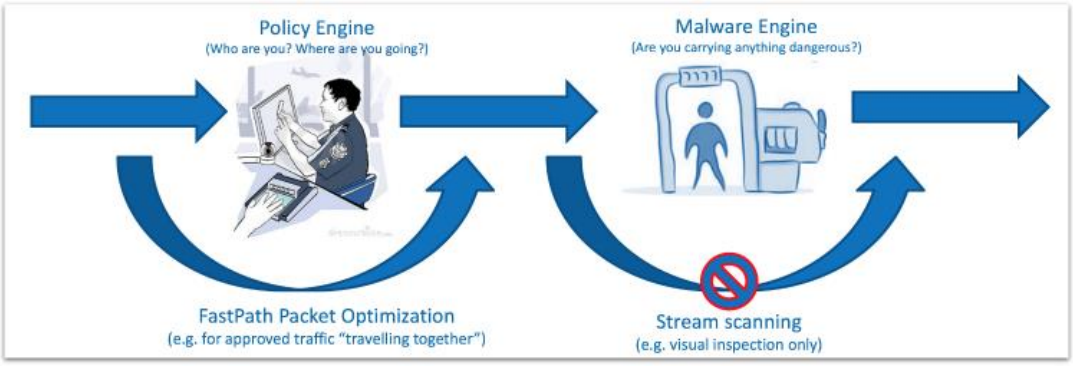
Laite	XG 550	XG 650
Palomuurin läpäisykyky	65 Gb/s	85 Gb/s
Palomuurin läpäisykyky sovellukset päällä	9 Gb/s	10 Gb/s
IPS läpäisykyky	17 Gb/s	20 Gb/s
VPN läpäisykyky	8,4 Gb/s	9 Gb/s
Istuntojen maksimimäärä	30 000 000	30 000 000
Uudet istunnot sekunnissa	220 000	240 000

4.4.1 Toimintatavat

Sophos XG -palomuurit tarjoavat hyviä ratkaisuja tietoturvan ylläpitämiseen. XG-sarjasta löytyy kaikki olennaisimmat seuraavan sukupolven palomuurin ominaisuudet. XG-palomuurin ominaisuuksiin kuuluvat muun muassa tunkeutujanestojärjestelmä, kehittynyt uhkasuoja, kaksi itsenäistä virustorjuntaa (Dual AV), sovelluskontrollointi sekä sähköpostisuoja. XG-palomuureissa käytetään Sophosin Synchronized Security -teknologiaa, joka muodostuu kahdesta osasta: Security Hearthbeatista ja Synchronized App Controlista. Security Heartbeat tarkkailee järjestelmän ja päätelaitteiden tilaa ja pystyy tarvittaessa vastaamaan turvallisuusuhkiin eristämällä järjestelmiä, kunnes tutkinta on suoritettu ja uhka poistettu. Security Heartbeatin tietoja voidaan tarkastella XG-palomuurin käyttöliittymässä, josta nähdään muun muassa uhkien määrä ja laatu. (Sophos 2017a, 1-2.) Synchronized App Control on Sophosin ratkaisu sovellustunnistukselle. Synchronized App Control antaa mahdollisuuden muun muassa tunnistaa ennestään tuntemattomia sovelluksia ja priorisoimaan tiettyjä sovelluksia säätelemällä kaistanleveyttä. Sophosin XG-palomuurien käyttöliittymässä sovelluksista voidaan saada paljon tietoja. Käyttöliittymästä voidaan saada selville esimerkiksi,

minkälaisissa päätelaitteissa sovellus on esiintynyt, kuinka monta kertaa sovellus on esiintynyt, milloin sovellus on viimeisen kerran esiintynyt ja minkälainen luokitustila sovelluksella on. Sovelluksille voidaan määritellä manuaalisesti kategorioita, jolloin palomuuri voi priorisoida sovelluksen liikennettä ennalta määriteltyjen sääntöjen mukaan. (Sophos 2017c.)

Sophos on optimoinut pakettien tarkastusta palomuureissaan FastPath-nimisellä tekniikalla. FastPathin tarkoitus on parantaa palomuurin läpäisykyvyn tehokkuutta ja alentaa viivettä. FastPath on ikään kuin ohituskaista, johon XG-palomuuri laittaa automaattisesti luetetut ja turvalliset paketit. Ohituskaistalle laitettujen pakettien ei tarvitse läpäistä palomuurin policy engineä identiteetin tai määränpään tarkastamisesti, vaan paketti välitetään suoraan security engineen tarkasteltavaksi. Pakettien turvallisuus ja luetettavuus todetaan esimerkiksi pakettien kuuluvan samaan sarjaan keskenään. Käytännössä palomuuri tarkastaa sarjan ensimmäiset paketit ja päästää loput tähän sarjaan kuuluvat paketit ilman tarkastusta läpi. Sophos vertaa FastPathin toimintaa lentokenttien turvatarkastuksiin kuvion 8 mukaan. (Sophos 2015.)



Kuvio 8. Sophosin hahmotelma FastPathin toiminnasta. (Sophos 2015)

Käyttäjätunnistus on toteutettu Sophosin omalla patentoidulla Layer-8 Identity Control -tekniikalla. Käyttäjätunnistuksen avulla voidaan määritellä käyttäjätason oikeuksia sovelluksille, määrittää kaistanleveyttä ja muita verkkoresursseja. Layer-8 Identity Control tekee käyttäjätunnistuksen riippumatta käyttäjän IP-osoitteesta, sijainnista, verkosta tai laitteesta. (Sophos 2017a, 2.)

XG-palomuureissa palosääntöjen tekeminen on helppoa. XG-palomuurit tarjoavat valmiita pohjia nopeaan ja sulavaan sääntöjen luomiseen. Valmiista sääntöpohjista löytyy esimerkiksi pohjat Exchangen ja Sharepointin ylläpitoon. Sääntöjä voidaan toki myös luoda uusia, eikä valmiita sääntöpohjia ole pakko käyttää. (Sophos 2016b.) XG-palomuurit osaavat luoda automaattisia riskianalyysejä käyttäjistä Sophos User Threat Quotientin

(UTQ) avulla. Palomuuri analysoi jokaisen käyttäjän surffaustapoja ja aktiviteetteja verkossa riskialttiin käytöksen varalta. (Sophos 2018.)

XG-palomuureissa on käytetty pilvipohjaista Sandboxing-tekniikkaa nimeltä Sandstorm. Palomuuriin saapuva paketti tutkitaan aluksi palomuurissa käyttämällä hyödyksi allekirjoituksia ja tutkimalla haitallisia URL-osoitteita. Jos tiedostoa ei todeta haitallisesti, palomuuri lähettää Sandstormiin tiivisteen tiedostosta tarkastettavaksi, onko Sandstorm aiemmin analysoinut vastaavanlaista pakettia. Jos tiedosto on aiemmin analysoitu, Sandstorm välittää tiedon palomuurille voiko tiedoston välittää eteenpäin käyttäjälle. Jos Sandstorm ei ole aiemmin nähnyt samanlaista tiivistettä, palomuuri lähettää kopion tiedostosta Sandstormille analysoitavaksi. Analysoinnin tuloksesta riippuen tiedosto välitetään käyttäjälle tai estetään. Sandstorm pystyy estämään esimerkiksi kiristyshaittaohjelmia, naamioituna ohjelmatiedostoja, PDF-tiedostoja ja Microsoft Office -dokumentteja. (Sophos 2016a.)

4.4.2 Lisenssit ja listahinnat

Sophos on jakanut XG-palomuurien lisenssipaketit neljään ryhmään. Nämä ryhmät ovat FullGuard Plus, FullGuard, EnterpriseGuard Plus ja EnterpriseGuard. Suppein lisenssivaihtovaihtoehto on EnterpriseGuard, joka sisältää työkalut tietoverkko- ja web-suojaukseen. Näihin suojaustapoihin kuuluvat tunkeutumisenestojärjestelmä, kehittynyt uhkasuoja (Advenced Threat Protection, ATP) ja Heartbeat, site-to-site VPN, ilman clientiä toimiva VPN, web-suojaus ja -kontrollointi, sovellussuojaus ja -kontrollointi sekä Web- ja sovellusliikenteen hahmottaminen. EnterpriseGuard Plus sisältää edellä mainittujen ominaisuuksien lisäksi myös Sophosin Sandstorm sandboxing-ominaisuudet. FullGuard-lisenssi sisältää EnterpriseGuardin ominaisuudet tuoden mukaan sähköposti- ja verkkopalvelinsuojauksen. Näihin suojiin kuuluvat sähköpostien kontrollointi, karanteenaus, salaus ja datan menetyksen esto (Data loss prevention, DLP) sekä verkkosovellussuoja (Web Application Firewall Protection). FullGuard Plus on laajin lisenssivaihtoehto, joka sisältää kaikki suojaustavat: Sandboxingin, tietoverkko-, web-, sähköposti- ja verkkopalvelinsuojan. (Sophos 2017b.) Lisenssit ja niiden sisältämät ominaisuudet on havainnollistettu taulukossa 12.

Taulukko 12. Sophos XG-palomuurien lisenssivaihtoehdot (Sophos 2017b, 6)

XG Firewall Features by Subscription Summary

Features (as listed above)		FullGuard Plus				
			FullGuard			
		EnterpriseGuard Plus				
			EnterpriseGuard			
	Base Firewall	Sandstorm Protection	Network Protection	Web Protection	Email Protection	Web Server Protection
General Management (incl. HA)	●					
Firewall, Networking and Routing	●					
Base Traffic Shaping and Quotas	●					
Secure Wireless	●					
Authentication	●					
Self-Serve User Portal	●					
Base VPN Options	●					
IPSec Client	Sold seperately					
Sandstorm Protection		●				
Intrusion Prevention (IPS)			●			
ATP and Security Heartbeat™			●			
Remote Ethernet Device (RED) VPN			●			
Clientless VPN			●			
Web Protection and Control				●		
Application Protection and Control				●		
Web and App Traffic Shaping				●		
Email Protection and Control					●	
Email Quarantine Management					●	
Email Encryption and DLP					●	
Web Application Firewall Protection						●
Logging and Reporting	●	●	●	●	●	●

Sophos myy myös TotalProtect ja TotalProtect Plus -paketteja, joihon sisältyy lisenssien lisäksi myös laite ja Plus-versiossa Sandstorm-sandbox. Yksittäisiä lisenssejä voi ostaa myös erikseen. Lisenssien uusiminen on myös suhteessa halvempaa kuin uuden lisenssin ostaminen.

Taulukko 13. Sophos XG 550 ja 650 -palomuurien listahinnat (EnterpriseAV 2018a) (EnterpriseAV 2018b)

Laitteen nimi	XG 550	XG 650	Voimassaoloaika
Laitteen listahinta	$ 12,445	$ 18,995	-
TotalProtect	$ 43,358	$ 66,179	3 vuotta
TotalProtect Plus	$ 54,111	$ 82,590	3 vuotta
FullGuard	$ 35,348	$ 52,426	3 vuotta
FullGuard Plus	$ 45,101	$ 68,838	3 vuotta
EnterpriseGuard	$ 19,414	$ 26,897	3 vuotta

4.5 Listahinnat ja kilpailutus

Edellä esiteltyihin palomuureihin etsittiin internetistä suuntaa antavat listahinnat. Tarkoituksena oli löytää itse palomuurilaitteen ja siihen myytävien lisenssien hinnat. Listahinnat eivät ole lopullisia ostohintoja. Lopullinen ostohinta syntyy eri laitetoimittajia kilpailuttamalla.

Listahintojen vertailua hankaloittaa eri laitevalmistajien erilaiset lisensointityylit. Huomattavin ero lisensoinnissa ilmeni Sophosin XG-laitteissa, joissa lisenssit oli jaettu karkeasti kahteen osaan. Molempiin näistä lisensseistä voidaan hankkia erikseen Sophosin Sandstorm sandboxing-linsenssi.

Laitevalmistajat myös myyvät lisenssejä eri mittaisille ajanjaksoille. Useimmiten lisenssin voi ostaa joko yhdeksi, kolmeksi tai viideksi vuodeksi. Osa laitevalmistajista tarjoaa myös erinäisiä pakettitarjouksia uusille laitteille. Näihin paketteihin voi kuulua esimerkiksi palomuurilaitteen muistin tai tallennustilan lisääminen tai erillisten moduulien ja lisenssien sisällyttäminen. Eniten yhdistelmäpaketteja tarjosi Check Point. Check Pointin palomuurilaite voidaan ostaa base-, HPP- tai max-rautakokoonpanolla, jonka ohelle voidaan ostaa myös samalla lisenssi.

4.6 Vertailu

Palomuurien vertailuun kilpailutusta varten huomioitiin kolme päätekijää. Ensimmäinen tekijä oli, että palomuurin tulee sisältää tietyt ominaisuudet. Toinen tekijä oli laitteen suorituskyvylliset ominaisuudet, kuten esimerkiksi kuinka paljon liikennettä palomuuri voi

päästää läpi tietoturvasovellusten ollessa päällä. Kolmas tekijä oli listahinta, jolla rajattiin budjettiin sopivat laitteet.

Kaikista vertailuun valituista laitteista löytyi halutut ominaisuudet, joita olivat esimerkiksi sovellustunnistus, käyttäjätunnistus, hyökkäyksenesto, antivirus ja sandboxing. Halutut ominaisuudet olivat tyypillisiä seuraavan sukupolven palomuureissa.

4.6.1 Suorituskyvylliset ominaisuudet

Toisessa vaiheessa verrattiin palomuurien suorituskyvyllisiä ominaisuuksia. Yksi tärkeimmistä asioista on palomuurin läpäisykyky. Läpäisykyky vaikuttaa merkittävästi liikenteen sulavuuteen ja siihen aiheutuvaan viiveeseen. Hidas verkko voi vaikuttaa yrityksessä negatiivisesti työtehokkuuteen tai mahdollisesti myös estää työnteon kokonaan. Myös liikenteen kasvava viive voi aiheuttaa aikakatkoksia päätelaitteiden ja palvelimien välillä. Väärin mitoitettu palomuuri voi aiheuttaa toteutuksesta riippuen joko suorituskyvyllisiä tai taloudellisia ristiriitoja. Alimitoitettu palomuuri voi aiheuttaa verkkoon merkittävän pullonkaulan, kun taas ylimitoitettu palomuuri aiheuttaa turhia kustannuksia kalliimman laitteen ja lisenssien takia. VPN:n läpäisykykyyn kannattaa kiinnittää erityisesti huomiota, jos verkon etäkäyttäjiä on paljon.

Taulukko 14. Palomuurien liikenteen läpäisykyky vertailussa.

Laitteen nimi	Palomuurin läpäisykyky sovellustunnistus päällä	Palomuuri kaikki sovellukset päällä	VPN:n läpäisykyky
Palo Alto PA-5220	18Gb/s	8 Gb/s	8 Gb/s
Cisco Firepower 4110	12Gb/s	10 Gb/s	6 Gb/s
Cisco Firepower 4120	20Gb/s	15 Gb/s	10 Gb/s
Check Point 15400	12,5Gb/s	7 Gb/s	10,8 Gb/s
Check Point 15600	17,5Gb/s	13,11 Gb/s	15,8 Gb/s
Sophos XG 550	Ei ilmoitettu	9 Gb/s	8,4 Gb/s
Sophos XG 650	Ei ilmoitettu	10 Gb/s	9 Gb/s

Taulukosta 14 voidaan todeta, että laitteiden läpäisykyvyt eivät laske samassa suhteessa toisiinsa nähden, kun kaikki tietoturvasovellukset on kytketty päälle. Tämä voi olla merkittävä tieto joissakin ympäristöissä, jos kaikkia ominaisuuksia ei oteta käyttöön. Vertailussa täytyy myös muistaa, että luvut ovat teoreettisia, joiden saavuttamiseen on käytetty optimaalista testausympäristöä, joka ei vastaa todellista organisaation palomuuriympäristöä. Cisco Firepower 4120 on kummassakin vertailusarakkeessa tehokkain palomuuri. Suhteellisesti eniten pudotusta tekee Palo Alto PA-5220 -palomuuri, jonka läpäisykyky laskee yli puolella kaikkien tietoturvasovellusten ollessa päällä. Sophos oli ainoa laitevalmistaja, joka ei ilmoittanut palomuurin läpäisykykyä ympäristössä, jossa on vain sovellustunnistus käytössä.

Liikenteen läpäisykyky palomuurissa vaikuttaa etenkin käyttäjien kaistanleveyteen. Kaistanleveyden ohella on tärkeää, että palomuuri pystyy myös käsittelemään kaikki meneillä olevat istunnot ja yhteydet. Taulukosta 15 voidaan todeta, että palomuurit käsittelevät istuntoja hyvin eri tavoin. Palo Alto PA-5220 käsittelee parhaiten uusia istuntoja maksimimääräänsä nähden. Tosin Palo Altossa istuntojen maksimimäärä on huomattavasti pienempi kuin useimmilla muilla laitteilla.

Taulukko 15. Palomuurien kyky käsitellä istuntoja verrattuna toisiinsa

Laitteen nimi	Istuntojen maksimi lukumäärä	Uudet istunnot sekunnissa
Palo Alto PA-5220	4 000 000	171 000
Cisco Firepower 4110	9 000 000	68 000
Cisco Firepower 4120	15 000 000	120 000
Check Point 15400	3,2 / 25 miljoonaa*	185 000
Check Point 15600	3,2 / 25 miljoonaa*	185 000
Sophos XG 550	30 000 000	220 000
Sophos XG 650	30 000 000	240 000
*Enimmäismäärä valmiiksi asennetulla / maksimi muistilla		

4.6.2 Hinta

Hinta on yksi merkittävimmistä asioista palomuurin valintaprosessissa. Lähtökohtaisesti tietoturvasta ei pitäisi koskaan tinkiä, koska verkkohyökkäyksien aiheuttamat haitat voivat olla arvokkaampia kuin hintavan palomuurin hankkiminen ja ylläpitäminen. Onnistunut hyökkäys järjestelmään ei välttämättä aiheuta vain taloudellista vahinkoa, vaan se voi aiheuttaa myös epäluottamusta yritystä kohtaan ja sitä myöden huonoa mainetta. Esimerkiksi asiakastietojen vuotaminen on yritykselle aina vakava asia.

Seuraavan sukupolven palomuurien hinnoissa on kaksi osa-aluetta, jotka ovat syytä ottaa huomioon. Ensimmäisenä on itse laitteen hinta. Palomuurilaitteissa voi olla valtavia hintaeroja valmistajien ja mallien välillä. Osa laitevalmistajista myy myös laitteitaan useilla eri komponenttikokoonpanoilla, joka tekee yhden mallin hintahaarukasta laajan. Usein kalliimmassa laitteessa on esimerkiksi enemmän muistia ja tallennustilaa. Esimerkiksi Check Point myy osaa palomuureistaan kolmella erilaisella komponenttikokoonpanolla.

Taulukosta 16 voidaan tarkastella vertailuun valittujen palomuurilaitteiden listahintoja. Huomattavaa on laitteiden suuri hintaero. Halvin vertailuun valittu laite on Sophos XG 550, joka on listahinnaltaan yli kymmenen kertaa halvempi kuin vertailun kallein laite Cisco Firepower 4120. Laitteiden keskihinta on noin 68 000 dollaria ja mediaanihinta 63 000 dollaria.

Taulukko 16. Laitteiden listahintoja

Laitteen nimi	Laitteen listahinta	Vaihtoehtoiset versiot
Palo Alto PA-5220	$ 61,951	-
Cisco Firepower 4110	$ 89,995*	-
Cisco Firepower 4120	$ 149,995	-
Check Point 15400	$ 63,000	$ 77,500 (HPP)
Check Point 15600	$ 79,000	$ 91,000 (HPP)
Sophos XG 550	$ 12,445	-
Sophos XG 650	$ 18,995	-

Toinen hintaosa-alue on lisenssit. Seuraavan sukupolven palomuuri menettää merkityksensä, jos laitteeseen ei osteta mitään lisenssejä. Useimpien laitevalmistajien palomuurilaitteet toimivat normaalin palomuurin tavoin, jos laitteessa ei ole voimassa olevaa lisenssiä.

Lisenssien hintavertailu on vaikeaa laitevalmistajien erilaisten lisensointityyppien takia. Osa laitevalmistajista tarjoaa jokaisen lisäominaisuuden ostettavaksi erikseen ja toiset myyvät lisenssejä vain osana sovelluskokonaisuutta. Kaikki vertailuun valitut valmistajat tarjoavat mahdollisuuden ostaa lisenssit pakettina, mutta vain Cisco ja Palo Alto Networks myy myös sovelluskohtaisia lisenssejään erikseen.

Esimerkkinä Palo Alto PA-5220:n kolmen vuoden yksittäisten lisenssien listahinnat ovat noin 21,649 dollaria kappaleelta. Vastaavasti Ciscon kolmen vuoden yksittäiset lisenssit maksavat Firepower 4110 -laitteessa 43 000-54 000 dollaria ja Firepower 4120 -laitteessa 72 000-90 000 dollaria.

4.6.3 Muut valintaan vaikuttavat kriteerit

Palomuurin valintaan voi vaikuttaa myös muut tekijät. Yksi merkittävä tekijä voi olla laitevalmistajan luotettavuus tai vahva brändi. Koska palomuuri on yksi tietoverkon tärkeimpiä laitteita, halutaan se usein hankkia tunnetulta yritykseltä, jolla on hyvä maine tietoturvapiireissä. Esimerkiksi pitkään tietoturva- tai verkkolaitealalla toimineet yritykset voivat olla huomattavasti uskottavampia kuluttajan näkökulmasta. Vähemmän tunnetut palomuurivalmistajat voivat kilpailla IT-alan jättiläisiä vastaan houkuttelemalla kuluttajia tarjoamalla huomattavasti halvempia laitteita kilpailukykyisillä ominaisuuksilla.

Isoimmista yrityksistä etenkin Cisco luotti markkinointimateriaalissaan vahvasti brändiinsä jättäen kertomatta syvällisemmin palomuurilaitteidensa toimintatavoista. Cisco mainitsi materiaaleissaan usein omistamiaan tuotemerkkejään kertomatta niistä yhtään tarkempia tietoja. Osaan tuotemerkityistä tekniikoista ei löytynyt mitään dokumentaatiota toiminnan suhteen.

4.7 Vertailutulos ja suositus

Vertailuun valituista laitteista suosittelisin erityisesti Palo Alto Networksin PA-5220-laitetta, joka nousee vertailussa sopivimmaksi vaihtoehdoksi muutamalla erityisellä seikalla. Palo Alto Networks kertoo sivuillansa ylivoimaisesti eniten palomuuriensa toiminnasta verrattuna kilpailijoihinsa. Useista ominaisuuksista löytyy oma PDF-tiedostonsa, jossa kerrotaan mitä kyseinen ominaisuus tekee, miten se toteutetaan ja mitä sillä saavutetaan. Useista ominaisuuksista kerrotaan yllättävänkin tarkkoja tietoja. Myös Palo Alto

Networksin taustat ja maine tietoturvayhtiönä vaikuttivat valintaan. Palo Alto Networks on yksi seuraavan sukupolven palomuurien markkinajohtajista, josta löytyy paljon käyttäjäkokemuksia internetistä. Palo Alton palomuureista löytyy myös huomattavasti paremmin opetusvideoita ja webinaareja internetistä. Useat näistä videoista kouluttavat Palo Alton palomuurisertifikaattien suorittamiseen. Tästä syystä Palo Alton palomuurit vaikuttavat lähtökohtaisesti käyttäjäystävällisimmiltä ja helpommilta ottaa käyttöön. Palo Alto PA-5220:n hinta on vertailuun valituista laitteista keskikastia. Vertailussa olleiden laitteiden keskihinta on noin 68 000 dollaria ja mediaanihinta 63 000 dollaria. PA-5220:n listahinta on noin 61,951 dollaria, joka alittaa sekä keksi- että mediaanihinnan. Palo Alton lisensointityyli helpottaa käyttäjää valitsemaan vain ne ominaisuudet joita tarvitaan. Suorituskyvyltään PA-5220 oli hieman keskivertoa huonompi optimaalisessa testiympäristössä. Palomuurien teknisissä tiedoissa olevien lukujen ylitulkinta voi tosin olla turhaa, koska laitteiden suorituskyky voi muuttua paljon monimutkaisessa ja realistisemmassa ympäristössä. PA-5220:ssa on myös todella hyödyllinen virtuaalipalomuuri-ominaisuus, jota ei mainittu muiden vertailuun valittujen laitteiden markkinointimateriaaleissa. Tämä ei kuitenkaan sulje pois mahdollisuutta, etteikö kilpailijoiden laitteissa olisi tätä ominaisuutta. Ominaisuus voisi käytännössä tulla laitteisiin laajemman ohjelmistopäivityksen myötä.

Vaihtoehtona Ciscon Firepower-laitteet kärsivät hyvin niukasta dokumentaatiosta, joka ei tarjoa lainkaan syvällisempää tietoa laitteiden toiminnasta tai ominaisuuksista. Ciscon markkinointistrategia vaikuttaa pohjautuvan heidän vahvaan brändiinsä verkkolaitealalla. Cisco Firepower -palomuurit olivat myös vertailun kalleimpia laitteita.

Check Point on tunnettu osaaja tietoturva- ja palomuurialalla. Vertailuun valitut laitteet Check Pointilta olivat kilpailukykyisiä sekä ominaisuuksiltaan että hinnoiltaan. Dokumentaatio palomuurien ominaisuuksista oli suhteellisen hyvää ja selkeää, mutta kaukana Palo Alton tasosta. Hintaluokassaan Check Pointin base-tason palomuurit sijoittuivat hyvin pitkälti keskikastiin. Parempien komponenttikokoonpanojen laitteet nousivat hinnoissa keskikastin yläpuolelle. Check Pointin sovelluspaketteihin perustuva lisensointi ei anna kuluttajalle paljoa valinnanvaraa, jos kaikkia ominaisuuksia ei haluta ostaa.

Sophosin suurin vahvuus on hinta. XG-sarjan palomuurit ovat hinnaltaan vain murto-osan heidän kilpailijoidensa hinnoista. Vaikka Sophos on tunnettu yritys virustorjuntaohjelmistoistaan, se ei ole erityisen tunnettu seuraavan sukupolven palomuureista. Sophosin palomuurien luotettavuudesta ei voi täysin varma, koska XG-

palomuurien käyttäjäkunta on huomattavasti pienempi kuin esimerkiksi Palo Altolla tai Ciscolla. Näin ollen käyttäjäkokemuksia näistä palomuureista on vaikeampaa löytää.

5 YHTEENVETO

Seuraavan sukupolven palomuurit ovat tulleet välttämättömäksi ratkaisuksi isojen lähiverkojen tietoturvan takaamiseksi. Verkkoliikenteen rakenteen muuttuminen on pakottanut palomuurien kehittymistä, koska pelkkien porttien, IP-osoitteiden ja protokollien avulla suodattaminen ei ole enää täysin luotettavaa. Suodattaminen on muuttunut sovellustunnistukseen perustuvaan tekniikkaan, jossa palomuuri tunnistaa erilaiset sovellukset verkkoliikenteestä. Sovelluksien toimintaa ja hyötykuormaa voidaan hallita. Palomuurit tunnistavat myös sovelluksien alisovellukset ja lisäosat, jolloin voidaan estää sovelluksista vain tiettyjä osa-alueita. Esimerkiksi pikaviestimissä voitaisiin sallia keskusteleminen, mutta estää tiedostojen lähetys. Myös verkkoliikenteen kasvanut salaus ironisesti luo uudenlaisia tietoturvariskejä, koska salatut paketit voivat sisältää haittaohjelmia. Seuraavan sukupolven palomuurit kuitenkin pystyvät purkamaan SSL-salauksia pakettien tarkastusta varten. Seuraavan sukupolven palomuurit tarjoavat myös palomuurisääntöjen luomisen käyttäjätasolla. Käyttäjätiedot haetaan usein toimialueen Active Directorysta tai RADIUS-palvelimelta, jolloin käyttäjä voidaan tunnistaa ilman IP-osoitetta. Tämä mahdollistaa, että käyttäjä saa samat palomuurisäännöt, vaikka hän olisi laitteellaan yhteydessä organisaation verkkoon langattomasti, langallisesti tai VPN:n avulla.

Tuntemattomat hyökkäykset ja haittaohjelmat ovat iso riski yrityksille. Vaikka tietoturvayhtiöt löytävät joka päivä uusia tartuntoja ja haittaohjelmia, on aina olemassa uusia riskejä, jotka ovat toistaiseksi tuntemattomia. Sandboxing-tekniikan avulla uusia tiedostoja ja ohjelmia voidaan ajaa eristetyssä turvallisessa ympäristössä, jossa tiedoston käyttäytymistä tutkitaan haitallisten toimintojen varalta. Jos tiedosto todetaan haitalliseksi, se tuhotaan. Suurimmat tietoturvayhtiöt tarjoavatkin seuraavan sukupolven palomuureihinsa erilaisia sandboxing-tekniikoita, jotka toimivat joko erillisessä laitteessa tai pilvessä.

Seuraavan sukupolven palomuurien kehittyneet ominaisuudet ovat maksullisten lisenssien alaisia. Laitevalmistajat myyvät lisenssejä esimerkiksi yhdeksi, kolmeksi tai viideksi vuodeksi kerrallaan.

Palomuurivertailu suoritettiin vertailemalla eri laitevalmistajien vaihtoehtoja Palo Alto Networksin PA-5220-palomuurille. Tähän vertailuun valittiin suorituskyvyiltään suurin piirtein samaa tasoa olevat palomuurit Ciscolta, Sophosilta ja Check Pointilta. Itse vertailussa huomioon otettiin palomuurien ominaisuudet ja niiden suorituskyky sekä listahinta.

Palomuurivertailun haaste oli, että eri laitevalmistajien laitteita oli yllättävän hankalaa vertailla toisiinsa. Laitevalmistajat painottavat omissa laitteissaan omia vahvuuksiaan ja patenttejaan, mutta samalla myös kertovat niiden toiminnasta yllättävän vähän. On vaikea todistaa, että tietyn laitevalmistajan tekniikka olisi paremmin toteutettu kuin kilpailijallansa. Vertailuun valituista laitteista suosittelisin erityisesti Palo Alto Networksin PA-5220-laitetta.

Yksi merkittävä syy Palo Alto Networksin PA-5220-laitteen valinnalle olivat valmistajan omat verkkosivut, josta löytyi todella kattavat dokumentit palomuurin ominaisuuksille. Palo Alton laitteista löytyy myös todella hyviä opetusvideoita ja webinaareja internetistä. Palo Alton palomuurit vaikuttavat tästä syystä käyttäjäystävällisimmiltä ja helpoimmilta asentaa omaan verkkoon. Vastapainona Ciscon materiaalit olivat huonoimmat epäselkeyden ja niukan tiedon takia. Hintavan palomuurin ostaminen ilman tarkempaa tietoa tuntuu itsestäni hieman epämiellyttävältä ajatukselta, vaikka laitevalmistaja olisi tunnettu alallaan.

Listahintojen vertailu perustui lähinnä hintahaarukan hahmottamiseen. Listahintojen vertailussa ilmeni kaksi ongelmaa. Ensimmäisenä ongelmana oli, että listahintoja oli ylipäätään vaikeaa löytää. Toinen ongelma oli, että laitevalmistajat käyttävät erilaisia lisensointitapoja laitteilleen, joten lisenssit eivät ole täysin vertailukelpoisia. Itse palomuurilaitteiden hintojen vertailu oli helpompaa. Hintahaarukka osoittautui varsin isoksi, sillä vertailun valitun halvimman ja kalliimman laitteen hintaero oli yli kymmenkertainen.

Suoritustehollisia ominaisuuksia vertaillessa laitteissa oli myös paljon hajontaa. Osalla laitteista oli paljon eroja suorituskyvyssä riippuen mitä ominaisuuksia on otettu käyttöön. Myös laitteiden tapa käsitellä paketteja vaikuttaa siihen paljonko ne voivat ylläpitää yhtäaikaisia istuntoja ja kuinka nopeasti.

Palo Alto Networks PA-5220 sai suosituksen olemalla kilpailukykyinen useammalla osa-alueella. Hintansa puolesta PA-5220 -laite on keskikastia. Ominaisuuksiltaan laite tarjoaa hyvät tavat liikenteen suodatukseen. PA-5220:sta löytyi myös virtuaalipalomuuri-ominaisuus, jota muut laitevalmistajat eivät maininneet omissa dokumenteissaan ollenkaan. Suorituskyvyltään PA-5220 oli hieman keskivertoa huonompi optimaalisessa testiympäristössä, joka ei välttämättä kerro koko totuutta palomuurin suorituskyvystä. Esimerkiksi palomuurin läpäisykyky voi muuttua paljonkin riippuen ympäristön rakenteesta, joten teknisissä tiedoissa olevien lukujen ylitulkitseminen voi olla turhaa. Palo Alto Networks on myös maineeltaan varma palomuurivalmistaja ja yksi markkinajohtajista.

Lähtökohtaisesti kaikkien isojen ja tunnettujen laitevalmistajien seuraavan sukupolven palomuurit ovat todennäköisesti luotettavia ja sisältävät kaikki tärkeimmät ominaisuudet

turvallisen ympäristön takaamiseksi. Suurimmat erot syntyvät suorituskyvyssä, hinnassa ja käytettävyydessä.

Pitää muistaa, etteivät seuraavan sukupolven palomuurit kuitenkaan voi estää kaikkia hyökkäyksiä tai taata täydellistä tietoturvaa. Paras tietoturva saavutetaan hankkimalla turvalliset, luotettavat ja hyvin konfiguroidut tietoturvalaitteistot ja päätelaitteet, sekä panostamalla verkon käyttäjien tietoturvakoulutukseen.

LÄHTEET

CDW 2018. Search Results [viitattu 2.2.2018]. Saatavissa: https://www.cdw.com/search/?key=pa-5220&searchscope=all&sr=1&pCurrent=1

Check Firewalls. 2018a. Check Point 15600 Security Appliance. [viitattu 23.4.2018]. Saatavissa: http://www.checkfirewalls.com/15600.asp?utm_source=vgsearch&utm_term=15600

Check Firewalls. 2018b. Check Point 15400 Security Appliance. [viitattu 23.4.2018]. Saatavissa: http://www.checkfirewalls.com/15400.asp#pricing

Check Point. 2016. Check Point Sandblast Network. Tietolomake [viitattu 23.4.2018]. Saatavissa: https://www.checkpoint.com/downloads/product-related/ds-sandblast.pdf

Check Point. 2017. Appliance Comparison Chart. Tietolomake [viitattu 6.4.2018]. Saatavissa: https://www.checkpoint.com/downloads/product-related/comparison-chart/appliance-comparison-chart.pdf

Check Point. 2018a. Anti-Bot Software Blade. [viitattu 23.4.2018]. Saatavissa: https://www.checkpoint.com/products/anti-bot-software-blade/

Check Point. 2018b. Check Point 15400 Next Generation Security Gateway for the Large Enterprise. Tietolomake [viitattu 23.4.2018]. Saatavissa: https://www.checkpoint.com/downloads/product-related/datasheets/ds-15400-appliance.pdf

Check Point. 2018c. Check Point Appliances. Tietolomake [viitattu 23.4.2018]. Saatavissa: https://www.checkpoint.com/downloads/product-related/brochure/br-appliances.pdf

Check Point. 2018d. Next Generation Threat Prevention Software Bundles. [viitattu: 23.4.2018]. Saatavissa: https://www.checkpoint.com/products/next-generation-threat-prevention/

Cisco Systems. 2018a. Advenced Malware Protection (AMP). [viitattu 5.4.2018]. Saatavissa: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html#~stickynav=2

Cisco Systems. 2018b. Cisco Firepower NGFW Data Sheet. [viitattu: 5.4.2018]. Saatavissa: https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/datasheet-c78-736661.html

Cisco Systems. 2018c. Compare Industry Next-Generation Firewalls (NGFWs). [viitattu: 5.4.2018]. Saatavissa: https://www.cisco.com/c/m/en_us/products/security/firewalls/competitive-comparison.html

Cisco Systems. 2018d. Licensing the Firepower System. [viitattu 23.4.2018]. Saatavissa: https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/licensing_the_firepower_system.html

Cisco Systems. 2018e. Next-Generation Intrusion Prevention System (NGIPS). [viitattu 5.4.2018]. Saatavissa: https://www.cisco.com/c/en/us/products/security/ngips/index.html

Davis, D. 2009. Routers, Switches & Firewalls – Learn how they are different. Petri IT Knowledgebase. [viitattu 5.4.2018]. Saatavissa: https://www.petri.com/csc_routers_switches_and_firewalls

EnterpriseAV. 2018a. Sophos XG 550. [viitattu 23.4.2018]. Saatavissa: http://www.enterpriseav.com/XG-550.asp#pricing

EnterpriseAV. 2018b. Sophos XG 650 [viitattu 23.4.2018]. Saatavissa: http://www.enterpriseav.com/XG-650.asp#pricing

Gregg, M. 2004. How do intrusion detection systems work?. TechTarget. [viitattu 5.4.2018]. Saatavissa: https://searchnetworking.techtarget.com/answer/How-do-intrusion-detection-systems-work

Humphreys, T. & Robertson, W. 2014. SSL Decryption – Using the Next Generation Firewall to eliminate Blind Spots. Palo Alto Networks. Video [viitattu 5.4.2018]. Saatavissa: https://www.paloaltonetworks.com/resources/webcasts/ssl-decryption-next-gen-firewalls

Infinity Technology Services. 2018. Palo Alto Firewalls Configuration by Example – PCNSE Prep – Deployment Options. Udemy. Video [viitattu 5.4.2018]. Saatavissa: https://www.udemy.com/palofirewalls/learn/v4/t/lecture/3496130?start=0

IT Price. 2018a. Cisco GPL 2018. [viitattu 23.4.2018]. Saatavissa: http://itprice.com/cisco-gpl/4120

IT Price. 2018b. Cisco GPL 2018. [viitattu 23.4.2018]. Saatavissa: http://itprice.com/cisco-gpl/4110

Li, Q. & Clark, G. 2015. Security Intelligence : A Practitioner's Guide to Solving Enterprise Security Challenges. [viitattu 5.4.2018]. Saatavissa: https://masto.finna.fi/Record/nelli16_phkk.3710000000496460

Marshall, C. & Ellis, C. 2017. The best free firewall 2018. TechRadar. [viitattu 5.4.2018]. Saatavissa: https://www.techradar.com/news/the-best-free-firewall

Messmer, E. 2012. SSL decryption may be needed for security reasons, but employees are likely to 'freak out'. Network World. [viitattu 23.4.2018]. Saatavissa: https://www.networkworld.com/article/2161439/network-security/ssl-decryption-may-be-needed-for-security-reasons--but-employees-are-likely-to--fre.html

Palo Alto Networks. 2016a. Content-ID. Tietopaketti [viitattu 5.4.2018]. Saatavissa:

https://www.paloaltonetworks.com/resources/techbriefs/content-id-tech-brief/

Palo Alto Networks. 2016b. User-ID. Tietopaketti [viitattu 5.4.2018]. Saatavissa: https://www.paloaltonetworks.com/resources/techbriefs/user-id-tech-brief.html

Palo Alto Networks. 2018a. Activate Licenses and Subscriptions. [viitattu 5.4.2018]. Saatavissa: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/activate-licenses-and-subscriptions

Palo Alto Networks. 2018b. App-ID. [viitattu 5.4.2018]. Saatavissa: https://www.paloaltonetworks.com/technologies/app-id

Palo Alto Networks. 2018c. Content-ID. [viitattu 5.4.2018]. Saatavissa: https://www.paloaltonetworks.com/technologies/content-id

Palo Alto Networks. 2018d. PA-5200 Series. Tietolomake [viitattu 5.4.2018]. Saatavissa: https://www.paloaltonetworks.com/resources/datasheets/pa-5200-series-specsheet

Palo Alto Networks. 2018e. Virtual Systems. [viitattu 5.4.2018]. Saatavissa: https://www.paloaltonetworks.com/features/virtual-systems

Rouse, M., Clark, C. & Cobb, M. 2018. Firewall. TechTarget. [viitattu 5.4.2018]. Saatavissa: https://searchsecurity.techtarget.com/definition/firewall

Rouse, M. & Shea, S. 2018. Next-Generation Firewall (NGFW). TechTarget. [viitattu 5.4.2018]. Saatavissa: https://searchsecurity.techtarget.com/definition/next-generation-firewall-NGFW

Sophos. 2015. Sophos XG Firewall innovations – FastPath packet optimization. [viitattu 6.4.2018]. Saatavissa: https://news.sophos.com/en-us/2015/12/10/sophos-xg-firewall-innovations-fastpath-packet-optimization/

Sophos. 2016a. How Sophos Sandstorm Works. Vimeo. Video [viitattu 6.4.2018]. Saatavissa: https://vimeo.com/156762603

Sophos. 2016b. Sophox XG Firewall – How it works. Vimeo. Video [viitattu 23.4.2018]. Saatavissa: https://vimeo.com/144094496

Sophos. 2017a. Sophos XG Firewall. Tietolomake [viitattu 6.4.2018]. Saatavissa: https://www.sophos.com/en-us/medialibrary/pdfs/factsheets/sophos-xg-series-appliances-brna.aspx

Sophos. 2017b. Sophos XG Firewall Features. Tietopaketti [viitattu 6.4.2018] Saatavissa: https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophosxgfirewallflna.pdf?la=en

Sophos. 2017c. Sophos XG Firewall Synchronized App Control. Vimeo. Video [viitattu 6.4.2018]. Saatavissa: https://vimeo.com/237000766

Sophos. 2018. Sophos XG Firewall. Tietolomake [viitattu 6.4.2018]. Saatavissa: https://www.sophos.com/en-us/products/next-gen-firewall/tech-specs.aspx

Suehring, S. 2015. Packet-Filtering Consepts in Linux Firewalls. InformIT. [viitattu 5.4.2018]. Saatavissa: http://www.informit.com/articles/article.aspx?p=2303307

Sweeney, p. 2012. Next-generation firewalls: Security without compromising performance. TechRepublic. [viitattu 9.4.2018]. Saatavissa: https://www.techrepublic.com/blog/it-security/next-generation-firewalls-security-without-compromising-performance/

Tech-FAQ. 2018. Firewalls. [viitattu 5.4.2018]. Saatavissa: http://www.tech-faq.com/firewall.html

Webroot Inc. 2014. What to do When Your Next Generation Firewall Protection Isn't Enough. Tietopaketti [viitattu 5.4.2018]. Saatavissa: https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/6214/5341/6981/what-to-do-when-your-next-generation-firewall-protection-isnt-enough.pdf

Wikipedia. 2018. OSI-mallin kerrokset. [viitattu 5.4.2018]. Saatavissa: https://fi.wikipedia.org/wiki/OSI-malli#/media/File:OSI-malli.jpg

Yeo, L. 2003. Choosing a Personal Firewall. InformIT. [viitattu 5.4.2018]. Saatavissa: http://www.informit.com/articles/article.aspx?p=31945&seqNum=3